Project Title	Wide – Impact cyber Security Risk framework
Project Acronym	WISER
Grant Agreement No	653321
Instrument	Innovation Action
Thematic Priority	Cybersecurity, Privacy & Trust, Risk Management, Assurance Models
Start Date of Project	01.06.2015
Duration of Project	30 Months
Project Website	www.cyberwiser.eu

D8.3 - PRACTICAL TOOLS FOR ASSESSING THE SOCIO-ECONOMIC IMPACT OF RISK MANAGEMENT IMPLEMENTATION FOR CYBER SECURITY, FINAL VERSION

Work Package	WP8, Go to Market
Lead Author (Org)	Alberto Biasibetti (AON)
Contributing Author(s) (Org)	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri, (TRUST-IT); Antonio Alvarez (ATOS)
Due Date	31.05.2017
Date	30.06.2017
Version	1.0

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

Versioning and contribution history

Version	Date	Author	Notes
0.1	03-03-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Initial analysis of case studies
0.2	03-04-2017	Alberto Biasibetti (Aon)	Updated case study analysis
0.3	14-04-2017	Alberto Biasibetti (Aon)	First round of internal editing
0.4	20-04-2017	Antonio Alvarez (ATOS)	Updated approach to section 4
0.5	21-04-2017	Antonio Alvarez (ATOS)	Contribution to section 4
0.6	24-04-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Updated cyber risk analysis
0.7	26-04-2017	Alberto Biasibetti (Aon) Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	New case studies included
0.8	28-04-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Revised risk assessment
0.9	02-05-2017	Alberto Biasibetti (Aon) Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Checkpoint for internal review
0.10	05-05-2017	Atle Refsdal (SINTEF)	1st Internal Review
0.11	08-05-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Response to 1st Internal Review
0.12	12-05-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Updated analysis with insertion of costs and EU report on impacts on EU SMEs
0.13	19-05-2017	Alberto Biasibetti (Aon)	Initial review of tool concept and design
0.14	26-05-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Takeaways for each section in relation to new tool content development
0.15	06-06-2017	Alberto Biasibetti (Aon)	2nd review of tool concept and design
0.16	12-06-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Final analysis and tool content, including new features
0.17	14-06-2017	Alberto Biasibetti (Aon)	Final review of tool and presentation
0.18	16-06-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Marketing plan, conclusions and next steps
0.19	21.06.2017	Antonio Álvarez (ATOS)	Internal review

0.20	22-06-2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Response to internal review
0.21	23.06.2017	Antonio Álvarez (ATOS)	Layout checks
0.22	23.06.2017	Atle Refsdal (SINTEF)	Final review
0.23	22.06.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Response to review
0.24	28.06.2017	Ales Cernivec (XLAB)	Final Review
0.25	28.06.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Response to review
0.26	28.06.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Final version for GA approval
1.0	30.06.2017	Antonio Álvarez (ATOS)	Submission to EC

Disclaimer

Table of Content

List of Tables

List of Figures

Executive Summary

The CyberWISER socio-economic impact assessment tool (CW-SEIT) is a practical, business-friendly tool developed within WP8, which coordinates the Go-to-market strategy of WISER. It is designed to help small businesses to adopt cyber risk management in the face of growing threats from increasingly diverse and complex sources.

WISER has revised its initial approach to reinforce its "go-to-market" strategy, specifically to significantly increase adoption of its tools and services by European businesses and to support portability to verticals other than the pilots, which are now the major objectives of WP8.

CW-SEIT V2.0 is a thoroughly revised version of V1.0 based on a new and updated analysis, interaction with SMEs and the need for a truly practical tool that strengthens the WISER go-to-market-strategy. As a result, new software enhancements have commenced for rollout of CW-SEIT V2.0 in late July.

Now, the main purpose of CW-SEIT is to offer a free tool to SMEs that strongly encourages them to conduct continuous risk management. The new concept behind CW-SEIT V2.0 is therefore to enable them to understand the potential impacts of a cyber-attack on their businesses, looking at direct financial losses (economic impact), tangible and intangible impacts (social impact), ranging from reputational damage to harm to citizens. At the same time, CW-SEIT V2.0 guides SMEs to the portfolio of CyberWISER service packages, helping them make informed decisions about which ones to use.

It is therefore important to clarify that the tool has a distinctive value proposition compared with impact assessments offered in CWE and CWL:

- CW-SEIT is a first entry point to cyber risk management as a first essential step towards making EU businesses more cyber secure.
- CW-SEIT is also designed as an educational tool also on raising awareness of cyber threats and on getting ready for the GDPR, where very low awareness and understanding has been noted.
- CW-SEIT is also suited to small IT teams in public administration, and can also be used by larger companies that need an initial guide to cyber risk management. While WISER intends to promote it as a first step to other CyberWISER services, it does not preclude repeated use of the tool, including by different members of staff within the same organisation. Indeed, this is strongly encouraged.
- Like CWL, CW-SEIT is a free tool, a teaser to more advanced CyberWISER service packages.
- Unlike CWE and CWP, CW-SEIT does not have a direct market value for WISER. Its purpose with regard to CWE and CWP is to underpin the go-to-market strategy by including these service packages in the new WISER Risk Management Checklist. It thus supports uptake of WISER.
- The new CW-SEIT questionnaire also supports portability to other verticals (WP7) by including data gathering exercises to identify businesses by sector, country and risk profiles as potential WISER leads.
- The CW-SEIT also features a teaser on the cost-benefit analysis developed for CyberWISER Plus.

D8.3 first provides an extensively updated analysis of the threat landscape, and then presents new SW developments for CW-SEIT V2.0. The new developments for CW-SEIT take place in the light of:

- new findings about cyber risks and their impacts on businesses.
- WISER direct feedback from SMEs, their awareness levels, human and financial resources.

D8.3 updates the drivers behind CW-SEIT, proposes and presents the new SW developments that better fit with the analysis of the risk landscape in the first part of this report and our direct interactions with SMEs. The approach is also aligned with the conclusions of the NIST Cybersecurity Framework Workshop 2017 (16-17 May), which highlighted the need for clear messages and practical resources for SMEs with regard to risk management[1].

The development of CW-SEIT V2.0 draws on the analysis of the cyber risk analysis, looking at current and forecast trends alongside case studies and statistics related to different economic and social impacts. A key finding is the multi-faceted, complex risk landscape, which is difficult for SMEs to navigate. Hence justifying a CW-SEIT V2.0 that offers practical guidance not only on risks but also to preparing for the forthcoming GDPR. The end result is a reinforced Go-to-market strategy for WISER.

WISER is highly motivated by its strong practical approach of its go-to-market strategy, where the main purpose of CW-SEIT is to:

1. Facilitate the implementation of cyber risk management amongst SMEs across Europe as crucial for IT security and also in view of the forthcoming GDPR.
2. Provide SMEs with a practical guide to CyberWISER service packages so they can select the services that are right for their business needs and IT budget.
3. Align the tool with the WISER Go-to-Market strategy and support portability to other verticals (WP7), including customer information gathering exercises.

D8.3 therefore also looks at why an SME would want to make sure it is cyber secure and why it should seriously consider the implications of not doing cyber risk management. It also provides insights into how WISER can help them prepare for new EU regulations, such as the General Data Protection Regulation, which comes into force in May 2018.

CW-SEIT is also useful for small IT teams in public administrations and for larger companies as a first approach to cyber risk management.

[1] https://www.nist.gov/news-events/events/2017/05/cybersecurity-framework-workshop-2017.

1. Introduction

1.1 Purpose and Scope

The overall aim of D8.3 is to show the pragmatic approach that WISER is taking to cyber risk management as an essential asset for businesses and public-sector organisations that depend on IT/computer software for their core business, operational efficiency, or added-value services.

Specifically, D8.3 reports on the final development of CW-SEIT. First, we provide an in-depth and updated analysis of the risk landscape through a set of case studies showing different impacts. We then provide an analysis of current and predicted trends before focusing on specific challenges for SMEs, looking at their increasing threat surface and current risk management practices. We also consider increasing costs of cybercrime for businesses and how these may rise with the upcoming EU legislation such as the General Data Protection Reform (GDPR).

Each of the above sections concludes with the main takeaways for WISER.

From this vantage point, we review the initial version of CW-SEIT and present its final development based on a decision-making approach, that also draws on the new analysis and direct feedback from SMEs across Europe. The section dedicated to the tool also considers marketing aspects for CW-SEIT and its positioning within the WISER product vision (D2.6).

1.2 Structure of the document

The document is structured as follows:

- The introduction defines risk assessment and socio-economic impacts, looks at the main drivers for SME risk management, and provides a sample of sources consulted.
- Section2 defines selected cyber threats and then presents a set of case studies illustrating different types of socio-economic impacts resulting from successful cyber-attacks while also showing new trends in the cyber threat landscape. It concludes with key takeaways for WISER based on key points emerging from the case studies.
- Section 3 analyses current and forecasted trends in cyberspace, looking also at typical threats in specific sectors. This is the basis for enhancements and updates to CW-SEIT, where the aim is to reflect the main findings as much as possible. It opens with an overview of the main findings shaping the enhancements to CW-SEIT while offering an example of how WP8 seeks to provide rapid at-a-glance overviews for the time-pressured business community.
- Section 4 examines business impacts based on an extensive review of the most recent and relevant reports. It also discusses the GDPR, business preparedness and implications for cyber risk management. It opens with an overview of the main findings shaping the enhancements to CW-SEIT while offering an example of how WP8 seeks to provide rapid at-a-glance overviews for the time-pressured business community.
- Section 5 is dedicated to CW-SEIT developments based on the new analysis and direct interactions with SMEs, with the aim of educating SMEs on the benefits of risk management and guiding users to CyberWISER service packages, practical guides and glossaries. It also presents the cost-benefit analysis as a basic approach to the service provided in CyberWISER Plus.
- Section 6 focuses on opportunities for WISER emerging from the analysis, positioning CW-SEIT within the portfolio of packages and presenting related WP8 Go-to-market timelines.
- Section 7 presents the conclusions and next steps.

1.3 Drivers for SME Risk Management

The Internet revolution is giving rise to a digitally-connected world with opportunities for innovation, creativity and new forms of social endeavour. However, the huge potential progress in economic and social life could be jeopardised by growing clandestine intrusion into digital systems. Cybercrime and inappropriate or unsanctioned use of digital information that defy geographical and jurisdictional boundaries.

Through T8.5 (socio-economic impact tool development), WISER seeks practical responses to cyber risk management in a complex, multi-faceted landscape, where SMEs are seriously ill-prepared to defend their business assets and protect their customers. CW-SEIT is designed to lower barriers to cyber risk management for SMEs, enabling them to assess the likely effects of a cyber-attack and reduce, as much as possible, those impacts. The tool is also useful for small IT teams in public administrations and large companies as a first approach to risk management.

From a WP8 perspective, key drivers for CW-SEIT are therefore:

- Raising awareness and educating SMEs on cyber risk management as the first fundamental step towards a better IT security posture, and which is becoming increasingly important as the GDPR approaches.
- Aligning the tool with the WISER product vision for its service packages: CyberWISER Light, CyberWISER Essential and CyberWISER Plus, and guiding CW-SEIT users to the best possible package for their needs and budgets.

1.4 Definitions: Risk Assessment and Socio-economic Impacts

We start by defining risk management and socio-economic impacts, including some key points to bear in mind in relation to assessing impact.

Risk Management

Risk assessment is essentially a tool for obtaining a consistent picture of risk knowledge already available implicitly or explicitly. Such knowledge can be sufficient for identifying grey swans even in today's complex and fast-evolving cyber threat landscape. There are also cases of high-consequence risk with low likelihood, which is a challenge within risk management in general. In *Cyber-Risk Management*, A. Refsdal et al draw a distinction between incidents that occur as complete surprises (black swans) and incidents that have far-reaching consequences but that can be anticipated to a certain degree (grey swans)[2].

An important challenge regarding cyber risk management is that cyberspace evolves rapidly and often in a manner that is difficult to predict. This requires increased focus on monitoring and risk assessment in real time as part of the overall cyber risk management.

A key point in the context of WISER is that cyber risk management is not an issue that concerns only IT and security professionals but the entire organisation, ensuring that it is part of the business processes for companies of all sizes, and board-wide in large ones. The overriding aim is therefore to help create a cyber security culture where businesses can manage their risks and have in place measures to protect their IT and their customers.

Socio-economic Impacts[3]

- **Economic impacts and knock-on effects:** the direct financial losses resulting from a cyber-attack, including also stolen money or financial data (e.g. credit cards); fall in market value, fines imposed by national or EU competent bodies (including regulators), as well as fines imposed by the forthcoming Network and Information Security Directive (NISD) and General Data Protection Regulation (GDPR). Indirect costs include loss of business and/or staff time

[2] A. Refsdal, B. Solhaug, K. Stølen, *Cyber-Risk Management*, Springer, November 2015.

[3] With respect to WISER socio-economic definitions in D3.5 Sections 11 and 12, D8.3 uses words and terms that small businesses and small IT teams in public administration can easily relate to, drawing also on external business guides on cyber security.

in fixing the problem (which may entail external expert support), loss of market/stock exchange value, loss of IPR, as well as reduced or lost ability to gain new business/contracts because of known past cyberattacks. Such impacts are often knock-on effects of direct impacts and may only become apparent over time.

- **Impacts on society:** intangible and tangible costs to society are wide-ranging and include damage caused by stolen highly personal health data, delayed medical treatment affecting patient health, risk of blackmail and other types of psychological stress, safety risks to all segments of society, reduced or lost reputation in the eyes of customers or the public, and erosion of trust in ICT.

Examples of stolen data include: names, email addresses, telephone numbers, dates of birth, hashed passwords, and even encrypted and unencrypted security questions and answers.

The use cases in section 2.2. provide clear examples of the different types of socio-economic impacts resulting from successful cyber-attacks.

Extracting the real-world impact of a cyber-attack is not always easy as we also have to factor in second or third order effects, which may not be apparent in the aftermath of a cyber-attack. Some impacts and subsequent risks surface over time, e.g. vulnerabilities may be exploited up to 12 months after being identified. In secondary attacks, hackers may use leaked details to target other organisations, such as credential stuffing, which exploits re-used passwords and user names to compromise other accounts.

The final costs to users may also be difficult to estimate as they depend on many factors, such as the success of follow-up phishing or fraud attempts. Breached data may be sold through the online criminal marketplace.

1.5 Rationale for Sources selected for analysis

There is a vast amount of academic, expert practitioner and stakeholder literature on cyber security, including specialised and general published media. As a whole, literature reveals the intricate and multidisciplinary nature of cyber security and a complex and evolving landscape of threats.

The focus of WISER WP8 is on communicating the importance of cyber risk management to the EU business community and on marketing the CyberWISER service packages. CW-SEIT centres on the economic and sociological impacts on EU businesses and small IT teams in public administrations, helping them take their first steps towards risk management and from there adapting effective cyber security products and services.

To achieve its go-to-market goals, WP8 must ensure its messages reflect the information needs of SMEs and small IT teams, who have a poor understanding of the cyber risks they are facing and few resources to manage them. To this end, WISER has carefully selected sources written primarily for the target users of CW-SEIT, whether that be governments, analysts or the media.

The table below provides a summary of the main sources selected.

Source	Date of Publication	Value Add for WISER Analysis
Cyber-Risk Management, A. Refsdal, B. Solhaug, K. Stølen, Springer 2015	November 2015	Risk management, cyber security, cyber-risk assessment, building on practices from industry.
Cyber Security Breaches 2016, HM Government report[4] (S1) Support from: Confederation of	May 2016	Details business actions on cyber security, costs and impacts of cyber breaches and

[4] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016.

British Industry, Federation of Small Businesses, ICAEW.		attacks.
Lloyds of London, Facing the Cyber Risk Challenge[5] (S2)	September 2016	Survey of almost 350 senior decision makers across Europe on current practices, including preparedness for the GDPR.
UK National Cyber Security Strategy 2016-2021 – HM Government[6] (S3)	November 2016	Sets out a new national plan for dealing with evolving cyber threats and their socio-economic impacts.
Cybersecurity in the European Digital Single Market – High level Group of Scientific Advisors N°2/2017[7] (S4)	March 2017	Provides policy context for revised EU Cyber Security Strategy, including recommendations.
The Cyber threat to UK business – 2016/2017[8] A joint report by the UK National Cyber Security Centre (NCSC) and National Crime Agency (NCA) (S5)	March 2017	Provides insights into the evolving cyber threat landscape and impacts on business community.
Hyperfinance Report - global law firm Simmons & Simmons[9]	April 2017	200 senior level respondents (30% at C-suite level) across five financial centres.
Industry Survey: Transformative Technology Adoption and Attitudes – Cybersecurity – ABB Research[10].	May 2017	Survey of 455 U.S.-based companies across nine vertical markets. Not available for free download but summarised in selected media channels.
Cybersecurity Framework Workshop 2017[11]	16-17 May 2017, 2017	Users' experiences that will help others in making effective use of the Framework and assist NIST in finalising Version 1.1. later in 2017.
Media reports on known cyber-attacks, spanning diverse sectors and geographies – referenced in footnotes. (various). Such sources have also been used to assess trends and	Period from December 2015 to May 2017	Specific threats and examples on socio-economic impacts, supplementing the WISER Case Studies Sources on SMEs include: Racconteur; small business.co.uk; The Guardian, as well as information from UK

[5] http://www.privacyrisksadvisors.com/news/lloyd-s-survey-facing-the-cyber-risk-challenge/.
[6] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
[7] https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf.
[8] http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file.
[9] http://www.simmons-simmons.com/en/news/2017/april/hyperfinance-research-uncovers-key-concerns-around-fintech-adoption-in-hong-kong-and-singapore.
[10] https://www.telecomtvtracker.com/insights/abi-research-b2b-technology-survey-finds-more-than-half-of-healthcare-respondents-not-concerned-with-cybersecurity-10244/.
[11] https://www.nist.gov/news-events/events/2017/05/cybersecurity-framework-workshop-2017.

impacts on SMEs.		reports.

Table 1: Summary of Sources Analysed

2 Cyber Threats and Case Studies

2.1 Types of Risks and Typical Damage

WISER interaction with SMEs (e.g. ClujIT Innovation Days in March 2017) showed a clear lack of knowledge of even the most basic of cyber-security related terminology amongst small businesses. This lack of knowledge is a key driver behind the basic glossary of cyber security terms made available on the WISER website, in English with partner translations into their national languages[12].

While a valid threat picture today may not be valid tomorrow, the table below aims to identify the most relevant threats in relation to CW-SEIT and its focus on increasing a cyber security culture within the EU business community.

Type of Cyberattack	Typical Damage Caused
DDOS – Distributed Denial of Service: This type of attack can be set up cheaply and easily, from almost anyone. DDoS attacks have been a threat for many years, and are one of the most popular weapons in a cyber criminals' arsenal. However, Kaspersky noted significant advances in DDoS attacks in the last quarter of 2016, lasting 292 hours (12.2 days), setting a record for 2016 with an increase of 108 hours in just a few months.	A DDOS attack causes an **interruption to an online service**. It can be costly in terms of lost business due to an outage and also damage to reputation. It's therefore imperative that businesses find an effective way to safeguard themselves from such attacks. More recently, ransomware type DDoS attacks have been identified with what appear to be higher potential impacts.
Mirai: malware turns networked devices running out of date versions of Linux into remotely controlled bots that can be used as a part of a botnet in large-scale network attacks. The last quarter of 2016 saw the first massive DDoS attacks using the Mirai IoT botnet technology, including attacks on Dyn's Domain Name System (DNS) infrastructure and on Deutsche Telekom, which knocked 900,000 Germans offline in November 2016.	Mirai primarily targets online customer devices such as remote cameras and home routers. New trends show widespread impacts. Attacks on Internet Service Providers in Ireland and UK have partly targeted home routers in an attempt to create botnets.
Ransomware: this type of attack is expected to be the most common in 2017, with over 100 types identified by CloudTweaks[13]. **Top ransomware vectors:** phishing; SMSishing; Vishing; Social media; Instant message; Drive-by; System vulnerabilities; Malvertising; Network propagation and Propagation through shared services[14].	Malicious software that locks down data unless a ransom is paid, hence the name. The amount and payment method may vary. Such an attack can affect productivity as it locks down user files while a unique decryption key is created and stored on a hacker's server. Victims who pay up quickly may actually give the hacker more confidence, encouraging them to find more and more unscrupulous ways to make money.
GoldenEye ransomware - is a new form	Evidence available suggests that GoldenEye is

[12] https://cyberwiser.eu/news/quick-multi-lingual-guide-glossary-cyber-security. It is interesting to note that the Slovenian media have picked up on the glossary as useful also for their understanding of cyberspace.
[13] http://ow.ly/VKmT30bhVWe.
[14] https://fightransomware.com/ransomware-articles/top-10-ransomware-attack-vectors/.

ransomware written by the same cybercriminal who gave us the Petya and Mischa ransomware attacks[15] with the same distribution tactics of masking the ransomware as job applications, swamping email inboxes. GoldenEye essentially performs the file encryption activities of Mischa and then restarts to perform the MFT encryption activity of Petya. Both encryption methods have been improved, and decryption methods for Petya and Mischa will not work on GoldenEye. Other new types of ransomware include the **New Star Trek themed malware**: "Kirk" malware acting as a Low Orbit Ion Cannon (LOIC) denial of service tool, using Monero as the ransom payment of choice. "Spock" is the malware decryptor[16].	currently targeting potential victims in German-speaking countries, but that could change at any moment[17]. The programme encrypts files and displays a ransom message. However, after the initial ransom message is displayed, GoldenEye restarts the machine and encrypts the Master File Table (MFT) and replaces it with a custom boot loader that shows the ransom message upon computer start-up. GoldenEye's ransom message instructs victims go to a URL on the dark web to obtain their decryption key. Victims will need the decryption code presented in the ransom message to pay the ransom.
Zero-day vulnerability is a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and can fix it. Cyber criminal's capability to morph their malware has outpaced the Antivirus industry's ability to keep up with new signatures.	Recent research reveals that 30% of malware attacks are zero-day exploits that cannot be identified by legacy antivirus (AV) systems because they have not been seen before. According to Cyber-Risk Management, many zero-day vulnerabilities are "grey swans". However, it is important to note that high-consequence risks with low likelihood is a family of challenges and that security relevant bugs may pop up even in mature software that has been in use for years and widely tested[18].
Customisable Industroyer malware is believed to be capable of harming electric power systems and other types of critical infrastructure in any country. It is also thought to be at the root of the attack on Ukrainian power supply, a pivotal attack reported in case study 3.	Malicious actors see critical infrastructure as prime targets. If motivated, attackers could launch disruptive, inhibitive and potentially damaging cyberattacks impacting everyone, from average citizens to government agencies.
Less sophisticated but equally effective attacks come in the form of **Dropping Elephant** and **Carbanak malware**. Dropping Elephant (also known as "Chinastrats" and "Patchwork") is used against a variety of high profile diplomatic and economic targets, generally caught through spear-phishing or watering hole attacks.	Overall, the activities of Dropping Elephant show that low investment and ready-made offensive toolsets can be very effective when combined with high quality social engineering[19]. The Carbanak malware marked the beginning of a new stage in the evolution of cybercriminal activity, where malicious users steal money

[15] In May 2016, previously defeated Petya ransomware returns not as a single ransomware, but in a bundle with another malicious payload – Mischa. They deploy attacks on different layers of the system and are used as alternatives. See https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/ and https://blog.malwarebytes.com/threat-analysis/2016/06/petya-and-mischa-ransomware-duet-p2/.
[16] https://www.theregister.co.uk/2017/03/17/star_trek_ransomware/.
[17] https://fightransomware.com/news/resume-ransomware-goldeneye-targets-hiring-managers-recruiters-hr/.
[18] Cyber-Risk Management, op cit., p. 126.
[19] https://securelist.com/the-dropping-elephant-actor/75328/.

The main feature of Carbanak malware is Persistence, where attackers see money, not data, as the primary target. It is also important to note that bespoke malware can be used (see Case Study 2).	directly from banks, and avoid targeting end users[20].
Bespoke malware	Bespoke malware can also be used to launch an attack – Case Study 2 Attack on Bangladesh Bank's Swift System, is one example (see Sec. 2.2.2).

Table 2: Cyber Threats

2.2 Case Studies

The outcome of increasing cyber-attacks is growing economic losses and intangible costs such as costs to society, e.g. reputational damage to business and individuals, psychological trauma, general feelings of insecurity, etc. Beyond these costs, there are also threats to safety, health, and fundamental rights to privacy. The costs to society could therefore be substantial. In some cases, the physical impact on thousands of citizens can bring home the very tangible effects that a cyber-attack can have.

The purpose of the case studies is twofold: 1) provide concrete examples of impacts and knock-on effects of a cyber-attack and 2) show how trends are evolving in an increasingly evolving threat landscape broadening the potential for damage across organisations of all types and sizes.
The case studies come from a variety of sources, including several pivotal cyber incidents that have changed the security landscape, where the aftermath or full impact was not felt until 2016; recent attacks with on-going investigations; sector-specific attacks (primarily healthcare) and attacks on SMEs. With regard to the latter, it is important to note that this group receives significantly less media attention than attacks on larger companies and public-sector organisations, which makes it hard to find detailed information despite the fact that small businesses are facing increasingly more cyber risks.

2.2.1 Case Study 1 – Talk Talk

SIGNIFICANCE: The attack demonstrates that, even within large cyber-aware organisations, vulnerabilities can persist. Their exploitation can have a disproportionate effect in terms of reputational damage and operational disruption. This particular attack attracted substantial media attention. Rapid reporting of the breach enabled law enforcement to respond in a timely manner, and both the public and government to mitigate the potential loss of sensitive data.
VICTIM: Talk Talk, UK telecommunications provider
INCIDENT; Talk Talk report a successful cyber-attack and a possible breach of customer data. Subsequent investigation determined that a database containing customer details had been accessed via public-facing Internet servers, with the records of approximately 157,000 customers at risk, including names, addresses and bank account details. On the same day, several TalkTalk employees receive an email with a ransom demand for payment in Bitcoins. The attackers detail the structure of the database as apparent proof that it had been accessed. TalkTalk's report of the breach helps the police, supported by specialists at the National Crime Agency, to arrest the main suspects, all based in the UK, in October and November 2015.
METHODOLOGY: The technique used by the attacker, called SQL Injection,[21] has been well

[20] https://www.kaspersky.com/resource-center/threats/carbanak-apt.
[21] SQLi, whereby an attacker can execute malicious SQL statement (aka malicious payload) that controls a web application's database server (aka relational database management system – RDBMS).

known in security circles for almost 20 years. SQL injection is well understood, defences exist and Talk Talk ought to have known it posed a risk to its data. On top of that the company also had two early warnings that it was unaware of. The first was a successful SQL injection attack on 17 July 2015 that exploited the same vulnerability in the webpages. A second attack was launched between 2 and 3 September 2015.
IMPACT: The incident cost Talk Talk an estimated £60m (€71.4m) and the loss of 95,000 customers, as well as a sharp drop in their share price. In October 2016, the ICO fined TalkTalk a record fine of £400,000 (€475,500) because it had failed to apply the "most basic cyber security measures". Failure to do so left its database vulnerable to an SQL injection attack after failing to apply a fix on a software bug that had been available for more than 3 years.
Sources: UK Strategy 2016-2021; various media reports, e.g. BBC[22]; The Guardian[23].

2.2.2 Case Study 2 - Attack on Bangladesh Bank's Swift System

SIGNIFICANCE: The attack was a tailored attack which exploited the bank's access to the SWIFT payment system, used to securely transmit information and instructions among financial institutions. As such the attack targeted global financial services infrastructure through a specific bank and it is likely that the attacker will attempt to use this technique against other financial institutions. Perhaps unsurprisingly, the number of criminal groups targeting SWIFT has increased in the wake of the Bangladesh Bank heist. A new version of the Dridex financial trojan was launched in June 2016 with enhanced features, including functions to identify payment platforms, such as SWIFT.
VICTIM: Bangladesh Bank
INCIDENT: In February 2016, $81m was stolen from Bangladesh Bank by targeting the bank's SWIFT system. BAE reported that bespoke malware was used to attack the bank's infrastructure which also had the capability to manipulate the Bangladesh Bank's legitimate internal SWIFT payment orders system. BAE released further analysis on 13 May which indicates that at least one other financial institution, in Vietnam, has been targeted by the same threat actor.
METHODOLOGY: A police investigation into the theft has stated that the bank's IT technicians may have connected its SWIFT international payments system to the Internet while setting up a connection to the bank's domestic payments system. The technicians reportedly also left a hardware token inserted in the server for months at a time, though it should have been removed and stored securely after business hours each day. Earlier findings from a Bangladesh government inquiry indicated failings such as technicians disabling anti-virus software and staff keeping a 'secret notebook' of login IDs and passwords on the system. The attackers injected six types of malware which captured keystrokes and screenshots. The investigators suspect that an insider at the bank provided the attackers with technical details about its computer network, as the malware was customised for the bank's system.
IMPACT: In December SWIFT, the global payment messaging system, warned users of an increased cyber threat to its systems, describing the threat as, very persistent, adaptive and sophisticated – and here to stay." This cyber heist was a significant attack because it targeted global financial services infrastructure, warning that the attacker or others are likely to repeat the success of the heist. It is one of the five pivotal game-changes in recent times.
FINANCIAL IMPACTS: Attempted fraud of US$951m (€874m). 30 transactions, worth US$850m (€782m), were prevented by the banking system. However, 5 transactions worth US$101m (€93m) went through. US$20m (€18m), traced to Sri Lanka, has since been recovered. The remaining US$81m (€74m) transferred to the Philippines was laundered through casinos and some of the

[22] http://www.bbc.com/news/technology-38223805;
[23] https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack.

funds were then forwarded to Hong Kong.
SOURCE(S): The Cyber threat to UK Business – 2016/2017 report

2.2.3 Case Study 3 – Destructive Attack on Ukrainian Power Supply

SIGNIFICANCE: This is a watershed incident in cyberspace, primarily because it's the first confirmed case of cyber-enabled disruption to electricity supply on a regional scale. Often when discussing cyber-attacks, it is difficult to extract the real-world impact, which tends to be a second or third order effect. However, in this case the physical impact on thousands of citizens brought home the very tangible effects that a cyber-attack can have.
VICTIM: Ukrainian energy distribution companies
INCIDENT: Three Ukrainian energy distribution companies were victim to cyber-attack in December 2015, resulting in electricity outages for approximately 225,000 customers across the Ivano-Frankivsk region of Western Ukraine. Attackers gained unauthorised entry into a regional electricity distribution company's corporate network and ICS. Subsequently seven 110 kV and twenty-three 35kV substations were disconnected for three hours. A recent article highlights that customisable malware known as Industroyer was likely to be at the root of the attack[24].
METHODOLOGY: Spear-phishing emails with malicious Microsoft Word attachments containing BlackEnergy 3 (BE3) malware. BE3 did not directly cause the outage, but rather was used to gain access to the business networks of electricity supply companies. Attackers reportedly gained access to networks more than six months prior to the December 2015 power outage. This was followed by the theft of credentials from corporate networks. The corporate VPNs and remote access tools were used to enter and manipulate ICS networks. KillDisk malware was then deployed to erase the master boot record on targeted systems and log deletion to hide presence on networks. In one instance, attackers launched a telephone DoS attack to delay customers reporting outages to the affected company's call centre.
IMPACT: Attackers overwrote the firmware on critical devices used by the affected companies, forcing operators to control devices manually, leading to a significant drop in productivity. The length of the power outages was limited because technicians on site manually overrode circuit breakers and restored power after a few hours. However, more than two months after the attack, control centres were still not fully operational.
SOURCE(S): UK Strategy 2016-2021 and the UK cyber threat to UK business – 2016/2017 report.

2.2.4 Case Study 4 – Historic Yahoo! Data Breaches

SIGNIFICANCE: Whilst this incident did not occur in 2016, it had significant impact that year for two reasons: 1) The scale. There are few incidents, in cyber or otherwise, that have the potential to impact such a large portion of the global population. This is likely to manifest itself through secondary attacks which use leaked details to target other organisations, such as credential stuffing, which exploits re-used passwords and usernames to compromise other accounts, and which is likely to have increased because of these breaches. 2) The cost. It is difficult to estimate the final cost to users whose accounts have been compromised, this will depend on many factors such as the success of follow-up phishing or fraud attempts. In business terms, after the revelation, the purchase price of Yahoo!'s core internet business by Verizon was reduced by US$350m (€322m) to US$4.48b (€4.48b). The decision could set a precedent for how cyber security can affect the valuation of an organisation.
VICTIM: Yahoo! and its customers
INCIDENT: In August 2013, data associated with one billion Yahoo! user accounts was accessed by an unauthorised party. Yahoo! believe the breach is distinct from another incident that occurred in 2014 which impacted 500 million user accounts. The stolen data reportedly included names,

[24] https://www.ciodive.com/news/industroyer-malware-behind-ukrainian-power-outage-capable-of-significant/444845/.

email addresses, telephone numbers, dates of birth, hashed passwords and in some cases, encrypted and unencrypted security questions and answers.
METHODOLOGY: Yahoo! stated that the 2013 breach occurred when an unauthorised third party stole data associated with accounts. Yahoo! has not been able to identify the intrusion associated with this theft. Out-side forensic experts are conducting an ongoing investigation into the creation of forged cookies that could allow an intruder to access Yahoo! users' accounts without a password. Yahoo! have connected some of this activity to the 2014 data theft.
IMPACT: Breached data is often sold through the online criminal marketplace. Personal data can be used by criminals to access other accounts held by the victim, or even to create convincing phishing emails. It is likely that some victims of the Yahoo! breaches have been targeted for phishing campaigns or identity fraud.
SOURCE(S): UK cyber threat to UK business – 2016/2017 report (op cit.); various media reports, e.g. The Guardian[25]

2.2.5 Case Study 5 – Public Release of The Mirai Malware Source Code

SIGNIFICANCE: DDoS attacks using botnets are not new. However, the rapid exploitation of the connected devices market to launch unprecedented, large and sustained attacks is a step change. The number of devices that could be recruited into a botnet has significantly increased and will continue to do so. Gartner estimate there will be 21 billion connected devices by 2020. It is highly likely that criminals will seek to monetise the Mirai botnet both in renting it out as a premium DDoS-For - hire service capable of launching notably large DDoS attacks in an otherwise crowded DDoS For - hire marketplace. The threat from the Mirai botnet is here to stay.
VICTIM: Multiple victims, including the Brian Krebs security website, network provider OVH, and internet performance management company, Dyn. Indirect victims included organisations such as PayPal and Twitter. UK telecommunications provider TalkTalk and Post Office customers also reported internet connectivity outage following Mirai router scanning activity.
INCIDENT: Mirai is the name of the malware currently infecting vulnerable, connected devices. It is also the name of the botnet made up of compromised connected devices. The source code for the Mirai malware was released to the public in October 2016, and has led to a significant lowering of technical barriers to entry in the launching of large, sustained DDoS attacks. The attack against Krebs was the largest on record to date with a peak attack size of 665 Gbps. The network provider OVH reportedly suffered multiple attacks exceeding 100 Gbps individually, which collectively resulted in a 1 Tbps attack.
METHODOLOGY: Mirai scans for 68 user name and password combinations when seeking to brute force, infect and control a connected device. Attackers issue commands to infected devices worldwide, which then direct internet traffic to overwhelm victim sites and disrupt service provision. Newer variants of Mirai have been seen to scan for vulnerabilities within routers as an alternative means of infection.
IMPACT: The immediate impact is disruption to services, which varies according to the capability of a victim to deflect attacks. In some instances, attacks have caused disruption to services regardless of DDoS mitigation in place. There are financial costs associated with disruption recovery, as well as reputational costs for organisations whose customers are affected during attacks. Interestingly, the owners of infected connected devices suffer minimal disruption, making it difficult to encourage them to take measures to secure their devices.
SOURCE(S): UK cyber threat to UK business – 2016/2017 report.

2.2.6 Case Study 6 – Recent Attacks with On-Going Investigations

[25] https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

2.2.6.1 Wonga Data Breach

More recently, a large pool of customers using financial services have been the victims of data breaches with significant impacts, as outlined below, where immediate impacts are analysed.

DATE AND VICTIM: April 2017. Wonga data breach, financial services[26].
SIGNIFICANCE: The attack is thought to be one of the biggest in the UK, far exceeding the TalkTalk breach (affecting 150,000 customers). The difficulties in establishing the extent of the damage caused by cyber intruders also underlines the challenges faced by many organisations after a data breach.
INCIDENT & METHODOLOGY: The short-term loan firm, Wonga, reports a serious data breach with attackers believed to have used the company's website as the access point. The breach affects 245,000 customers in the UK and 25,000 in Poland. Data affected may include: customer names, email addresses, home addresses, phone numbers, the last four digits of customers' card numbers and/or bank number and sort code. While full card details are not thought to be at risk, even incomplete sets of financial data could put affected customers at risk of financial damage. Customers have been advised to change their account password, check for unusual activity and avoid passing on confidential information via email or phone calls, as well as be wary of unsolicited phone calls and emails.
IMPACT: The Information Commissioner's Office (ICO) is investigating the breach, methodology and causes. It will impose a fine if the company is found not to have taken adequate steps to keep customer data safe. Damage to society includes insecurity over personal and financial data, sense of insecurity.
SOURCE(S): The Guardian[27]; BBC[28].

2.2.6.2 WannaCry Ransomware Attack in May 2017

VICTIMS: Public and private sector organisations worldwide.
SIGNIFICANCE: Cyber-attack on unprecedented scale affecting over 200,000 computers in 150 countries. Experts believe another attack could be imminent. It was an indiscriminate attack across the world on multiple industries and services. International co-operation is seen as key for the scale of the cybercrime with Europol working with the FBI.
INCIDENT AND METHODOLOGY: Ransomware-type attack with software blocking access to data until ransom is paid combined with a worm application, a programme that replicates itself in order to spread to other computers. The virus exploits a vulnerability in Microsoft Windows software, first identified by the US National Security Agency. The ransomware is designed to spread infection across computers. It is also hard to guard against as it is easy for the initial hackers or "copy-cat authors" to change the virus code.
IMPACT: In England, 48 National Health Service (NHS) trusts reported problems at hospitals, GP surgeries or pharmacies, and 13 NHS organisations in Scotland were also affected, causing impacts on society. Other organisations affected include: some units in Nisson and Hitachi in Japan; problems with petrol station payment systems at Chinese energy giant PetroChina; Germany's rail network Deutsche Bahn, Spanish telecommunications operator Telefonica, US logistics giant FedEx and Russia's interior ministry. While economic impacts are slowly beginning to emerge, the full impact is hard to predict in the immediate aftermath. Hackers have demanded payments of around €270 in virtual currency Bitcoin to unlock files and return them to the user, but have issued threats to increase costs and delete files within 7 days. According to BBC analysts, approximately €345,810 had been paid a few days after the attack but is expected to rise. Many firms had experts working over the weekend to prevent new infections. It is also important to note that updating computers is much easier when the number is small. For organisations like the

[26] http://ow.ly/MjYH30bhVBq.
[27] https://www.theguardian.com/business/2017/apr/09/wonga-data-breach-could-affect-250000-uk-customers;
[28] http://www.bbc.com/news/business-39544762.

NHS, updating is time-consuming, expensive and complex.
SOURCE(S): various media sources, e.g. WIRED[29]; The Telegraph - Technology[30].

2.2.6.3 Adylkuzz Attack

VICTIMS: potentially any organisation that does not keep machines up to date with patches through updates[31].
SIGNIFICANCE: The most significant single global cyberattack yet, with potentially much more significant effects than WannaCry.
INCIDENT: The cyber-attack began in mid-May 2017, working quietly in the background as attention remained focused on the WannaCry attack
METHODOLOGY: The new variant of Adylkuzz appears to be stealthier than earlier versions. Rather than destroying assets in computers, it is using the machine to mine crypto keys and turn it into something with monetary value. The malware consumes resources such as CPU cycles, creating an army of machines (worm), with each one running a programme in the background linking up other machines infected and creating small amounts of cryptocurrency. These programmes go mostly unnoticed with effects that are not immediately obvious but that could potentially expand into something more malicious.
IMPACT: further media reports are pending at the time of writing.
SOURCE(S): various media reports

2.2.7 Case Study 7 - Sector Specific Attacks

The healthcare sector has long been “cyber insecure”. According to ABI Research, millions of health records have been breached since 2010. Ransomware is high on the list of threats and over 50% of global targets have targeted the sector in the past two years despite warnings from security experts. Here we look at the known impacts of cyber incidents in the first quarter of 2017.

2.3.1.1 Malware Attack on German Hospital Facilities

SIGNIFICANCE: The incident is symptomatic of economic impacts and impacts on society when a healthcare facility suffers a cyber-attack. The healthcare industry faces its own unique set of cyber security challenges as it is pushed by multiple compliance and regulatory requirements but also under pressure to cut costs while improving patient outcomes. Digitisation is a double-edge sword. On one hand, it improves patient care and overall efficiency. On the other, it may increase risk exposure as by storing more individual healthcare data in more places and on more devices.
VICTIM: Lukas Hospital in Neuss, Germany[32].
INCIDENT & METHODOLOGY: In February 2017, the hospital suffered a Ransomware DDoS attack on its IT system. Almost immediately the hospital reports the cyber incident to Germany’s State Criminal Investigation Office for advice on how to deal with an anonymous email address to stop the ransomware, which had taken control of the IT system.
IMPACT: Damage caused is both economic and societal. At the time of the incident being made public, the hospital had been without email access for over 3 weeks. Business as usual means using pen, paper and fax machines while IT professionals work to disentangle the system’s network. A considerable back log of notes to be entered into the EMR system has been another effect. Impacts to society include the delay of certain surgeries, and could also include potential loss of data not backed up before the attack.
SOURCE(S): Various media reports, e.g. ZDNet[33].

[29] http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017.
[30] http://www.telegraph.co.uk/technology/0/ransomware-does-work/.
[31] See, for example, http://www.abc.net.au/news/2017-05-18/adylkuzz-cyberattack-could-be-far-worse-than-wannacry:-expert/8537502.
[32] http://www.beckershospitalreview.com/healthcare-information-technology/2-weeks-into-ransomware-lockdown-german-hospital-awaits-instructions-from-hackers.html.
[33] http://www.zdnet.com/article/cybercriminals-hold-german-hospitals-to-ransom/. See also,

2.3.1.2 Attacks on UK Healthcare Sector

SIGNIFICANCE: Cyber incidents have been foreseen for some time yet research shows that much of the advice has been disregarded or due to the inability to make considerable updates to computer software. The incident also highlights the dangers of complacency in risk mitigation. They are also indicative of the increasing value of personal information for cybercriminals. Medical data can be used for ransom, while the data garnered through personal information such as email addresses and date of birth can be used to scam individuals.
VICTIMS: Hospitals, health clinics and teaching hospitals across the UK caused by 3 attacks in January, March and May 2017[34], [35].
INCIDENTS: Attacks variously affected East and North Hertfordshire NHS trust, Barts NHS trust, Essex Partnership university NHS trusts, the university hospitals of Morecambe Bay NHS foundation trust, Southport and Ormskirk hospital NHS trust, and Blackpool teaching hospitals NHS foundation trust, while GP surgeries across Liverpool and parts of Greater Manchester. The latest attack has involved co-operation with the National Cyber Security Centre, the Department of Health and NHS England to support affected organisations, ensure patient safety and recommend appropriate mitigations.
METHODOLOGIES: Large-scale global ransomware campaign sparked by leaked NSA exploit; zero-day vulnerabilities and the WannaCry attack (section 2.2.6.3).
IMPACT: Diversions of emergency patients. Problems with email systems, clinical and patient IT systems were also reported. The latest attacks have caused more extensive damages, such as various services including Accident & Emergency (A&E) affected across the country, clinics having to go back to paper records and cancelled appointments for several days. Impacts have been extensive, not only reduced capacity but also significant impacts on society. Like many public healthcare services, the UK's National Health Service (NHS) is already under pressure to maintain front-line services so incidents on this scale could have very high impacts on society including loss of confidence in public services and erosion of trust in IT.
SOURCE(S): Computer Weekly[36]; TelecomTV[37].

2.3.1.3 Online banking cyber-attack

Banks represent a high risk/reward proposition. Often the information they hold is easily converted into cash and some of the information literally is cash taken from compromised bank accounts transferred to offshore tax havens or unfriendly nations. Other information, such as addresses, phone numbers, emails, bank statements and in the US social security numbers (SSN) can be sold on the black market. Banks tend to have a great deal of investment in cyber protection, increasingly so in the light of high-profile attacks affecting the sector.

SIGNIFICANCE: Highlights vulnerabilities of bank IT systems that have high impacts on society especially when they are unacceptably frequent, and sometimes serious, exposing the public to the risks of IT banking failures, including delays in paying bills, an inability to obtain their own money,

http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030.

[34] http://www.computerweekly.com/news/450418720/NHS-hospitals-hit-by-suspected-ransomware-attack?utm_content=control&utm_medium=EM&asrc=EM_ERU_77281762&utm_campaign=20170518_ERU%20Transmission%20for%2005/18/2017%20(UserUniverse:%202373947)&utm_source=ERU&src=5635922.

[35] http://www.telecomtv.com/articles/healthcare/healthcare-organisations-notoriously-lax-over-computer-security-charge-researchers-15631/.

[36] http://www.computerweekly.com/news/450418720/NHS-hospitals-hit-by-suspected-ransomware-attack?utm_content=control&utm_medium=EM&asrc=EM_ERU_77281762&utm_campaign=20170518_ERU%20Transmission%20for%2005/18/2017%20(UserUniverse:%202373947)&utm_source=ERU&src=5635922.

[37] http://www.telecomtv.com/articles/healthcare/healthcare-organisations-notoriously-lax-over-computer-security-charge-researchers-15631/.

and unauthorised access to their accounts.
VICTIM: HSBC
INCIDENT: In January 2016, HSBC customers were locked out of internet banking (internet and mobile) for several hours. Customers (17m personal banking and business customers in the UK) were unable to log into their accounts until late in the afternoon on a day when many employees received their first pay packet of the year. The bank worked with CERT-UK (the government-backed Computer Emergency Response Team) to help identify the criminals responsible.
METHODOLOGY: Distributed Denial of service attack overwhelming the bank's online banking service, taking it offline. A DDoS can often be often used as a smokescreen drawing away the attention of information security teams in the financial institution from the real intent, e.g. large value money transfers, bulk threat and removal of customer account data.
IMPACT: Evidence shows that information was not stolen but that the incident was associated with high impacts on society. The driver behind such attacks can be related to the public image of the institution and consumer goodwill towards it with the intention to harass, intimidate and embarrass the targeted institution in the short term.
SOURCE(S): The Guardian[38].

2.2.8 Case Study 8 – Attacks on SMEs

In recent years, the average SME has gone from using predominantly simple siloed solutions to embracing more interconnected systems. From bring your own device (BYOD) to off-site working in the cloud, small businesses have never been more connected to their clients and more open to threats.
SMEs have not been a traditional target of cyber-attacks. Yet, according to Symantec, the percentage of attacks targeted at SMEs (less than 250 employees) increased from 18% in 2011 to 43% in 2015, while attacks against very large companies (2500 or more employees) decreased from 50% to 35% in the same period. Such a trend shows not only that SMEs are increasingly becoming attractive targets but also face the same risks as large companies. A key difference being that a cyber-attack on a small business could mean they go under. According to one estimate, 60% of small firms go out business within 6 months of a cyber-attack[39].

SIGNIFICANCE: The incident shows how devastating clicking a malicious email can be on a small business. It is highly indicative of SMEs being totally unprepared for a cyber breach due to a lack of awareness of the magnitude an attack can have – in this case almost threatening the entire company.
VICTIM: MNH Platinum – vehicle hire company
INCIDENT: In early 2015 MNH Platinum became the victim of a virus that encrypted over 12,000 files on it company network with a payment demand of £3,000 (€3500) to decrypt the files. As the virus proved impossible to remove without loss of critical company data, the firm paid the ransom fee.
IMPACT: High economic impact for an SME, which was only able to retrieve documents crucial to running the business.
SOURCE(S): The Guardian[40].

[38] https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack.
[39] https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html. See also, http://www.yorkshirepost.co.uk/news/three-out-of-every-four-smes-have-been-hit-by-cyber attacks-1-8295143.
[40] https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses.

Infected email attachments and malicious competitor actions (scenario from HM Government, Small Businesses: What you need to know about cyber security**)**
SIGNIFICANCE: a small manufacturing company loses an important contract as a rival company with hostile intentions uses information collected over time against it.
METHODOLOGY: The attackers used social media sites to identify key employees and get information from them about locations, contact details and current work projects. Armed with this information, the adversary sent targeted and realistic-seeming emails to a number of staffs in different teams, containing attachments infected by malware. They also stole a work laptop from the managing director on a business trip. The attacker used malware capability together with the stolen laptop to get into the network and extract vital information about the company and its contract bid. They used this to produce a rival bid at lower cost, using stolen intellectual property.
IMPACTS: The company lost out on the contract. Without this work, it was impossible to maintain the full workforce and half of the employees were made redundant. This news was picked up by the local media, leading to lasting reputational damage and further loss of business.
SOURCE(S): HM Government, Small Businesses: What you need to know about cyber security[41] (latest update March 2015).

The cases below provide an indication of impacts of key trends on SMEs.

Ransomware Attacks
SIGNIFICANCE: 36% of ransomware victims report loss of business income due to the attack. This type of cyber-attack is expected to increase at least 300%.
METHODOLOGY: Cyber criminals are targeting SMEs in a growing number of ways. Ransomware attacks are proving to be the most popular methods used to extract money.
IMPACTS: The impact of a successful attack on hard-won reputation, supply chains and operations can be catastrophic for an SME.
SOURCE(S): Raconteur articles tailored to business communities[42].

Threats to IoT Devices
SIGNIFICANCE: 2016 was the year when cyber criminals shifted their focus to connected devices such as network security cameras and building control systems that can be controlled remotely over the Internet: 310% increase in the volume of attacks seeking out IoT devices between the first and final quarters of 2016. By the end of the year, over 90% of cyber-attacks on UK businesses targeted the control of connected devices in the workplace.
METODOLOGY: Most Internet cyber-attacks are computer scripts that search the web for weaknesses and probe firewalls constantly for a way in. The IoT means businesses are punching holes in their own firewalls to provide suppliers with access on their networks, which can open the door to criminals if not done properly.
IMPACT: Once inside, it is easy for hackers to take over connected devices and lie dormant before misusing assets as part of a bigger hack or DDoS attack at a later stage. It is therefore imperative that companies make their firewall policies as restrictive as possible by prioritising security over convenience.
SOURCE(S): small business.co.uk[43].

[41] https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know.
[42] https://www.raconteur.net/business/time-for-bosses-to-sit-up-and-take-notice-of-cyber-security. See also, https://www.raconteur.net/infographics/wannacry-the-biggest-ransomware-attack-in-history.

2.3 Main Takeaways for WISER

Intelligence gathered from the Case Studies:

- Complex and fast-evolving landscape broadening the potential for damage across organisations of all types and sizes. The UK cyber threat to UK business – 2016/2017 report highlights several pivotal attacks that have changed the security landscape, with some attacks being "very persistent, adaptive and sophisticated". The rapid exploitation of the connected device market to launch unprecedented, large and sustained attacks is a step change. Hackers are increasingly after monetary value.
- The public availability of some types of malware has already led to a significant lowering of technical barriers to entry to launching large sustained DDoS attacks.
- Attacks like the Talk Talk one show that vulnerabilities can persist, including widely known vulnerabilities, in even large, cyber-aware organisations with significant economic impacts (fines, reduced share price) and reputation damage leading to loss of customers.
- Impacts: some financial costs and on society (tangible and intangible) impacts are immediately obvious, while other impacts can be long lasting. When dealing with socio-economic impacts, it may sometimes be difficult to extract real-world impacts as they tend to be a second or third order effect. In some cases, impact depends on successful follow-up phishing or fraud attempts.
    - The immediate impact is typically disruption to services, which varies according to the capability of a victim to detect and deflect an attack. In some instances, attacks have caused disruption to services regardless of DDoS mitigation in place.
    - Many organisations face significant challenges in determining the extent of damage caused by cyber intruders as several factors may be involved.

Implications on risk management from the case studies

- The very recent WannaCry attack shows that very few countries worldwide are immune to a cyber-attack, which means that businesses in all EU countries need to remain vigilant and ensure that everyone in an organization has responsibility for ensuring data is adequately protected. Recent attacks have generally also caused more extensive damage and higher impacts on society than previous attacks.
- Risks and consequences of a cyber-attack are particularly high for critical infrastructures, healthcare facilities and financial institutions. This is also due to the value of the data they hold and further opportunities to scam customers, patients and medical staff.
    - In the healthcare sector, warnings about risks have been largely ignored. This is also because it is updating large numbers of computers is time-consuming, expensive and complex. The key question is whether healthcare facilities can continue to ignore risk management and cyber security investments.
    - Banks represent a high risk/reward. They tend to have a great deal of investment in cyber protection but are still vulnerable as cyber criminals become more sophisticated and as strong drivers remain in terms of harassing and intimidating the victims in the eyes of their customers.
- In the case of an SME, a successful attack damaging hard-won reputation, supply chains and operations can be catastrophic.
- Interestingly, the owners of infected connected devices suffer minimal disruption, making it hard to encourage them to take measures to secure their devices.

[43] http://smallbusiness.co.uk/smes-targeted-cyber-criminals-2536150/.

In the following section, we assess the current and forecast threat landscape to infer risks and related impacts on European businesses, especially SMEs. We look both general trends and Internet-enabled innovation opportunities that also pose increasing cyber threats.

3 Threat Landscape: Trends and Forecasts

3.1 Main takeaways for WISER

The wide-ranging analysis made for D8.3 shows that:

- Anyone can hire or be a cybercriminal and sophisticated attacks do not always require sophisticated cyber attackers. The impact of a cyber-attack (e.g. ransomware, DDoS) can be disproportionate to the technical skills of cybercriminals. UK examples include the Netspoof stresser that targeted gaming providers, government departments, internet hosting companies, schools and colleges, causing considerable disruption.
- Sophisticated attacks don't require sophisticated actors. For example, Carbanak malware exploiting old MS Office vulnerabilities do not require the same kind of sophisticated and high investments needed to uncover zero-exploits, or to develop advanced, modular cyber espionage platforms customised to attack targets.
- Cybercrime is becoming more aggressive. In some areas, e.g. parts of the UK, cybercrime is now more prominent than traditional crime types.
- Increase in cyber extortion through DDoS attacks, ransomware and data extortion.
- Ransomware remains the most common cyber extortion method.
- More ransomware incorporating locker techniques to counter mitigation efforts, such as preventing the downloading decryption tools.
- As the ransomware market matures, new strains will increasingly have unusual features to attract media attention.
- Higher ransoms are usually (but not exclusively) linked to the means to pay or particularly valuable data to the victim.
- Shift towards targeting specific businesses with high rewards.
- All digital businesses are potentially vulnerable as attack targets, whether they are a Fortune 500 company, a family-run business or a utility company. They will therefore need much more focused approaches to cyber risk management.
- Innovative FinTech firms with high market value can also benefit from new business partnerships. At the same time, they are potential attack targets and therefore need to protect their business assets and increase their security posture.
- Hospitals are an increasingly popular attack target either as a source of revenue by encrypting crucial data and demanding ransom for its release or as a source of valuable personal data of patients.

3.2 Current Trends

While many factors amount to a significant cyber threat to EU businesses and public-sector organisations, three features characterise current cyber threat trends.

Technical expertise is no longer necessary to carry out attacks.	The number of individuals capable of launching a cyber-attack now that malware and DDoS service-type models are easily acquired on the dark web.
The broader attack surface is increasing opportunities for attackers.	The attack surface and number of devices that can be used to launch attacks is expanding as the number of Internet connected devices grows. The most well-known example of this is the Mirai botnet, but the phenomenon also affects mobile devices and wearables as well as ICS (Industrial Controlled Systems) and other automated systems.
Threat actors are learning	The lines between different threat actors is blurring as

from and using one another's skills and capabilities.	individuals and groups learn from, hire and work with one another. Attacks on financial institutions are also coming from imitated suspect nations and more advanced actors are using "off the shelf" malware to launch attacks.

Table 3: Characteristics of Cyber-attacks

These factors represent a significant risk, where today's cyber criminals can directly steal money, monetise their capabilities indirectly through intellectual property theft, through extortion (e.g. ransom demands) or through malware.

Other trends are summarised in the table below.

Increase in Internet of Things botnets - exploiting security flaws in internet-connected webcams, CCTV, digital video recorders, smart meters and routers, which rose in 2016. Threats come from internet-connected devices that are part of the IoT, vulnerable to remote code execution or remote takeover. A large number of insecure devices can easily be found online, e.g. 41,000 units of one insecure model of DVR are connected to the internet as of 2017 as revealed by the Shodan search engine, all vulnerable to malware. An insecure device can be used to interfere with otherwise inaccessible products. Insecure devices can easily be recruited into a botnet that can then be used to mount DDoS attacks on an overwhelmingly large scale. In October 2016, a DoS attack on Dyn (domain name system company) caused severely restricted access for users. The incident took offline websites such as Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest, as well as newspapers such as the Guardian, New York Times and Wall Street Journal. This is just one example of the damage caused by IoT botnets[44] with more incidents expected in the near future and possibly on a larger scale[45].
Mobile Threats – expected to become part of the attack chain targeting consumers and organisations[46]. Malicious apps that initially manifest as a nuisance, e.g. delivering excessive adverts (adware), which are increasingly also requesting elevated permissions. This method could be used to install further malware such as key-loggers used to steal log-in credentials. Fake apps mimicking a brand or organisation to trick user into downloading them and entering credentials that are then stolen. 2016 saw the emergence of fake business enabling apps such as email and media sharing apps though most do not make it onto legitimate app stores. SMS phishing or SMishing is usually more effective than traditional PC phishing campaigns due to lack of awareness and implicit trust in the personal nature of SMS messages. A malicious SMS with a spoofed TPOA (the SMS header field that contains the message sender's number) will appear in the correct conversation thread, making it even harder to spot as a SMishing attempt. The Mobile Messaging Fraud Report 2016 found that 58% of the 6,000 consumers surveyed received an unsolicited SMS message every week, with 1/3 reporting that the message tried to trick them into disclosing personal data[47].
Social media as an attack vector - Malicious actors exploit social media as an environment of trust and familiarity. The abuse of trust has become the primary mechanism for starting an attack, as social engineering thrives on social media. Employees using social media could click on links from social media connections, with the same risks as opening links in phishing emails. Professional networking sites are particularly prone to malicious behaviour. Social media accounts are also used as command

[44] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.
[45] https://www.forbes.com/sites/kalevleetaru/2016/10/31/the-dyn-ddos-attack-and-the-changing-balance-of-online-cyber-power/#58e7476c3666.
[46] An in-depth analysis on security risks and requirements in 5G networks has been made by the 5G PPP Security Work Group, http://5gensure.eu/files/5g-pppwhite-paperphase-1-security-landscapejune-2017pdf.
[47] https://mobileecosystemforum.com/mobile-messaging-fraud-report-2016/.

and control (C2) infrastructure. Security researchers have discovered malware campaigns that use Twitter and Instagram, showing that it is easy for C2 channel traffic to appear normal in multiple, daily interactions.

3.2.1 Opportunities for FinTech to improve Cyber Security

Financial technology (FinTech) innovation is an important driver to expand access to financial services for large numbers of consumers ("democratising access to finance"). Europe has been at the forefront of FinTech[48].

According to Dow Jones VentureSource, venture capital investment in European FinTech companies reached its one its highest levels in Q1 of 2014[49], when FinTech companies raised a total of €166m (+21% compared to the previous quarter), a peak never seen in the industry since 2000. Leading countries include the UK, Germany and Spain[50]. More recently, Sweden has become a FinTech hotspot in the last two years. According to the Nordic FinTech Analysis published in January 2017, 1 in 3 FinTech investments are Swedish, including Stockholm-based payments companies Klarna (valued at $2.25bn; €2.25m) and iZettle ($500bn; €458bn).

New opportunities are expected to come from greater demand for customer personalisation and easy-to-use digital services as existing one-size-fits-all approaches come under sustained pressure. Personalisation through artificial intelligence and deep learning will be a key trend for the FinTech sector, affecting e-commerce, FinTech and all other services dependent on an internet user experience.

At the same time, these opportunities increasingly make FinTech companies high value/reward businesses with IT resource constraints like most other digital SMEs.

Interestingly, three-quarters of large global financial service companies have identified the importance of partnering with FinTech firms to help make the shift away from legacy IT systems and adopt innovative technologies (Hyperfinance Report, April 2017)[51]. 31% of the banks and asset managers surveyed expect to acquire a FinTech firm within the next 18 months. More collaboration between established financial institutions and FinTech firms has the potential to generate new investments over the next 12 months, including direct investments and collaboration with venture capitalists. One example of significant investments is US investment bank JP Morgan Chase is making a $9.5bn (€8.7bn) investment in technology including $600m (€550m) on small fintech companies during 2016, which was part of the reason for the company's success.

However, research also highlights the importance of addressing data protection and financial regulation obligations as these are making data sharing with third parties more difficult and may hinder the adoption of innovative technologies. Just under half the institutions see regulatory risks as too high, while others wish to wait longer to make sure of the right acquisition.

Key findings are:

- 71% of established institutions see cyber security as an associated risk in partnering with FinTech firms.
- Most large financial services firms believe better visibility of cyber security controls within FinTechs would improve prospects of partnering with them.

3.2.2 Healthcare and Embedded Medical Devices

While healthcare tends to be very slow to adopt new technologies because of regulations and liabilities, increasing digitisation means greater exposure to cyber risks, where electronic health

[48] https://startupxplore.com/en/blog/fintech-startups-europe/.
[49] https://www.fnlondon.com/articles/venture-capital-fintech-investment-hits-post-dotcom-high-20140428.
[50] http://tech.eu/features/8845/state-of-european-fintech-report-2015/.
[51] https://hyper-finance.com/app/uploads/2017/04/SimmonsSimmons-Hyperfinance-Report-INT.pdf.

records (EHR) contain a trove of personal data, making them an ideal target of one-stop hacking for cyber thieves. Other risks come from the growing use of IoT devices in healthcare facilities.

The healthcare industry is plagued by a myriad of cybersecurity-related issues. These issues range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care. While other critical infrastructure sectors experience these attacks as well, the nature of the healthcare industry's mission poses unique challenges. For healthcare, cyber-attacks can have ramifications beyond financial loss and breach of privacy[52].

And more and more hacking incidents are targeting medical devices. This is partly because they are easy targets. A non-trivial portion of exposed healthcare systems still use outdated operating systems, which can make them vulnerable. For example, more than 3% of exposed devices still used Windows XP, the retired Microsoft operating system that no longer receives security updates.

Unlike desktop computers and servers that run anti-virus software and other "endpoint" security checks, the diversity of IoT devices and initial lack of concern about their role in network security often makes them trivial to compromise. In one currently used exploit, known as MedJack, attackers inject malware into medical devices to then fan out across a network. The medical data discovered in these types of attacks can be used for tax fraud or identity theft, and can even be used to track active drug prescriptions, enabling hackers to order medication online to then sell on the dark web[53].

A new wave of ransomware attacks is disrupting access to digital systems and then demanding ransom in exchange for releasing the services so they can operate normally again. The effectiveness of holding to ransom hospital data or systems lies in the urgency to regain control. Hospitals face losing not just money, but critical resources for keeping patients alive.

In March 2017, Barts NHS trust was hit by an attack that exploited a zero-day vulnerability. In October 2016, three hospitals run by the Lincolnshire and Goole Foundation Trust were forced to cancel patient appointments and shut down systems for repairs after a ransomware attack. While the affected systems were reportedly restored without paying any ransom to cyber-attackers, the events further underline the importance of cyber security at healthcare organisations and raised renewed fears about NHS legacy IT systems, which have materialised in the recent WannaCry attack.

Wireless connectivity, remote-monitoring and near-field communication tech allow health professionals to adjust and fine tune implanted devices without invasive procedures[54]. However, many types of implanted medical devices are broadly vulnerable to attack, reducing the benefits of new features and technologies. British and Belgian researchers have identified security flaws in proprietary communication protocols of 10 new-generation Implantable cardiac defibrillators (ICDs). A key challenge lies in the fact that the proprietary code on these devices means it takes painstakingly reverse-engineering the software (like the researchers did for implantable cardiac defibrillators) for anyone outside a manufacturer to even assess the security of a device, much less discover flaws.

3.3 Horizon Scanning on Future Trends

3.3.1 Emerging Threat Landscape

The table below summarises the main future trends identified.

Ransomware	The emergence of open source ransomware programmes on GitHub and hacking forums is expected to further spur the growth of these attacks in 2017. Alternatively, cyber criminals without the skills to create their own malware can

[52] https://www.cisecurity.org/cyber-attacks-in-the-healthcare-sector/. Concerns were also confirmed at recent healthcare events, e.g. UK eHealth Week.

[53] https://www.theregister.co.uk/2017/03/13/thousands_of_nhs_staff_details_lost_in_breach_of_it_contractors_server/.

[54] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/, February 2017.

	outsource it with the ransomware as a service (RaaS) model, which provides automatically generated ransomware executables. The emergence of self-propagating ransomware with the same kind of characteristics traditionally found in network worms, such as Conficker is also on the list of predictions. This will result in a breed of ransomware designed to produce endless duplicates of itself, spreading the infection across an entire network. All businesses will be vulnerable as attack targets, whether they are a Fortune 500 company, a family-run business or a utility company, and will therefore need much more focused approaches to cyber risk management[55].
Internet's Building Blocks	Some of the most impactful attacks are expected to be directed at the building blocks on which the Internet runs, rather than innovative technology. In use of IoT devices to launch the Mirai botnet was innovative but its impact came from targeting part of the Internet's critical infrastructure. Domain Name Servers providers translate human readable domain names into internet addresses, acting as the phonebook of the Internet; this helps users find the websites they are looking for. There are many critical internet services, other than DNS, including website hosting, email, database servers, authentication and authorisation. Whilst they are not all vulnerable to the same attack methodology as DNS, a successful attack on one could have an equally far reaching impact. Rather than attacking a single website an attacker could target an upstream provider critical to the functioning of an organisation, such as DNS. An attack on upstream services would affect many organisations, serving to obfuscate the actual target or other simultaneous attacks.
Attacks on industrial connected devices will continue to increase	As more industrial systems become connected, the risk of an attack greatly increases. It is expected that connected devices in industry are already targeted and that incidents are more common than currently reported or detected. It should be noted that connecting services and devices can have unexpected consequences, especially in industries that have not previously had to consider cyber security risks. A representative case includes Finland, 2016, denial of service conditions disabled residential automated heating systems in apartment buildings for more than a week. Risk potential: While connected devices often provide tangible competitive and business advantage, the risk of connecting devices may be difficult to assess. There may be an increase in high-profile incidents that impact businesses because of lax security in connected devices. Victims of such attacks could be smart meters, networked security

[55] http://www.computerweekly.com/news/450410530/Ransomware-expected-to-dominate-in-2017?utm_medium=EM&asrc=EM_EDA_70777940&utm_campaign=20170109_UKCloud%20cuts%20cloud%20storage%20pricing%20for%20public%20sector%20customers&utm_source=EDA.

	cameras and connected indoor LED lighting.
Beyond encryption and data leaks to tampering with data	An attack on the integrity of data is particularly dangerous when the victim is unaware of it. Using an integrity attack against software to create VPN (virtual private network) backdoors has considerable downstream effects, weakening security in customer networks, which could be the hacker's intention. The success of this technique may encourage similar methods in 2017, and could impact numerous industries beyond IT. Research in late 2016 showed that it is possible for relatively unsophisticated actors to change online flight bookings (Security Research Labs). Damage includes cancelled or rebooked flights, as well as stolen passenger reward miles as effects on citizens and thus as impacts on society.

Table 4: Overview of Future Trends Identified

3.3.2 Berkeley Scenarios

The European Cyber Security Organisation (ECSO[56]) has recently highlighted the scenarios defined by the University of California, Berkeley as a valid approach for its member-driven association in shaping future work on the evolving risk landscape[57].

The scenarios are not intended as predictions but as future possibilities, exploring how emerging and unknown forces could intersect to reshape the relationship between humans and technology, and what being "secure" means as a result[58]. They form the basis for future research.

The Cyber Security Futures 2020 focus on:

- **The New Norm**: After years of mounting data breaches, Internet users in 2020 now assume that their data will be stolen and their personal information broadcast. Law enforcement struggles to keep pace as larger-scale attacks continue, and small-scale cyberattacks become entirely commonplace—and more personal[59].
- **Omega**: Data scientists of 2020 have developed profoundly powerful models capable of predicting—and manipulating—the behaviour of single individuals with a high degree of accuracy. For those responsible for cybersecurity, the stakes have never been higher[60].
- **Bubble 2.0**: Two decades after the first dot-com bubble burst, the advertising-driven business model for major internet companies falls apart. As overvalued web companies large and small collapse, criminals and companies alike race to gain ownership of under-priced but potentially valuable data assets[61].
- I**ntentional Internet of Things**: In 2020, the Internet of Things (IoT) is a profound social force that proves powerful in addressing problems in education, the environment, health, work productivity, and personal well-being. Because the IoT is everywhere, cybersecurity becomes just "security" and essential to daily life[62].
- **Sensorium (Internet of Emotion)**: In 2020, wearable devices won't care about how many steps you take; they will care about your real-time emotional state. Whether for blackmail,

[56] https://www.ecs-org.eu/.
[57] ECSO Meeting, June 2017, attended by Trust-IT.
[58] https://cltc.berkeley.edu/scenarios/.
[59] https://cltc.berkeley.edu/scenario/scenario-one/.
[60] https://cltc.berkeley.edu/scenario/scenario-two/.
[61] https://cltc.berkeley.edu/scenario/scenario-three/.
[62] https://cltc.berkeley.edu/scenario/scenario-four/.

"revenge porn," or other motives, cybercriminals and hostile governments find new ways to exploit data about emotion[63].

4 Business Impacts and Risk Management Practices

In this section, we present the main findings related to the business and financial impacts of cyber-attacks, especially for SMEs, the role of risk management in preparing for the GDPR, current risk management and reporting practices as a stark reminder that SMEs still have a long way to go before they are cyber secure.

4.1 Main Takeaways for WISER

The sources analysed by WISER show that SMEs are facing increasing cyber threats, highlighting the need for practical approaches to risk management, also in view of the GDPR. However, most SMEs remain unprepared for many of the potential new dangers of the cyber world, and are not ready for the GDPR. Instead of seeing security measures as a burden, it is vital SMEs treat them as an indispensable necessity[64].

4.1.1 Threats to SMEs

- An article by Racconteur focuses on the threat exposure of SMEs: "A cyber-attack on a smaller enterprise is unlikely to get anywhere near the level of publicity garnered by the hacking of a multinational corporation, but this doesn't mean there aren't many successful attacks against small firms on a daily basis. Many small businesses are starting to appreciate the potential severity of cyber-attacks. But many still have a long way to go in implementing good risk management"[65].

- The number of attacks on UK businesses reached 1000/day between November and December 2016, double the number of attacks since 2015, reaching 230,000 cyber-attacks[66]. Typical risks include CEO fraud, DDoS, and malicious software. Business assets attractive to cybercriminals span customer data, intellectual property, as well as access to larger companies to whose IT systems they are linked through business partnerships. Hackers take advantage of the lower defences of SMEs compared with larger companies[67].

Source: Juniper Research 2016

[63] https://cltc.berkeley.edu/scenario/scenario-five/.
[64] These figures are from a survey of 1,300 senior professionals, from small business to enterprise level, conducted by B2B International, in 11 countries, covering both developed markets, including the UK, USA and Japan and developing markets, including Brazil, China and India. See: Kapersky Lab, 'Ready or not? Balancing future opportunities with future risks. A global survey into attitudes and opinions on IT security', http://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf, 2015.
[65] https://www.raconteur.net/technology/why-smes-are-big-targets-for-cyber-crime.
[66] http://smallbusiness.co.uk/smes-targeted-cyber-criminals-2536150.
[67] https://www.racconteur.net/technology/why-smes-are-big-targets-for-cyber-crime.

Figure 1: Risk Awareness - UK example

- Relatively few companies (34%) have rules specifically around personal data encryption, which has been at the centre of various high-profile cyber security breaches. Businesses are also failing to factor in knock-on effects/indirect impacts of a cyber breach.
- According to Cyber Security Breaches 2016 (HM Government), many businesses have not taken appropriate actions around cyber security such as health checks, risk assessments and audits.
- SMEs usually have markedly different priorities than larger corporations, such as maintaining a strong cash flow and ensuring the right mix of skills and expertise is retained within their small teams. These pressures all mean that cyber risk is often not seen as a critical business risk by SMEs. But one thing that links SMEs to large organisations is they are equally at risk to cyber-attack – no one is immune. One small business, Accounting for Growth, states: "We take cyber risks very seriously, but as a small business we have so many different priorities to contend with, which means cyber issues are not always at the top of the list. The problem is businesses do not take it that seriously until it's too late or you hear that it's affected someone you know". Hence, they need practical tools they can use to understand the importance of risk management in mitigating to some extent the socio-economic impacts.

4.1.2 Financial impacts on EU businesses

- Companies spend an average of $880,000 (€784,000) in the aftermath of incidents. Disruption to normal operations can cost an average of $955, 400 (€811,000). Network downtime for SMEs is estimated to cost at least $20,000 (€17,800) an hour[68].
- While 58% of small businesses are concerned about cyber-attacks, 51% are not allocating any budget at all to risk mitigation: 38% of businesses surveyed regularly upgrade software solutions, 31% monitor business credit reports and 22% encrypt databases. 75% of small businesses have no cyber risk insurance[69].

'Measuring Financial Impact of IT Security on Businesses' (2016) by Kaspersky shows that the financial impact of cyber breaches can increase by as much as a factor of four when undetected for seven days, compared to the cost of it being detected instantly, as showed in the figure below based on a survey of 4,000 business representatives from 25 countries[70].

[68] https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html.
[69] https://www.racconteur.net/technology/why-smes-are-big-targets-for-cyber-crime.
[70] http://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf. Cited in Building an Effective European Cyber Shield - Taking EU Cooperation to the Next Level, May 2017, https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

While costs are significantly higher for large businesses, costs could be life-threatening to SMEs. The figure below comes from the report.

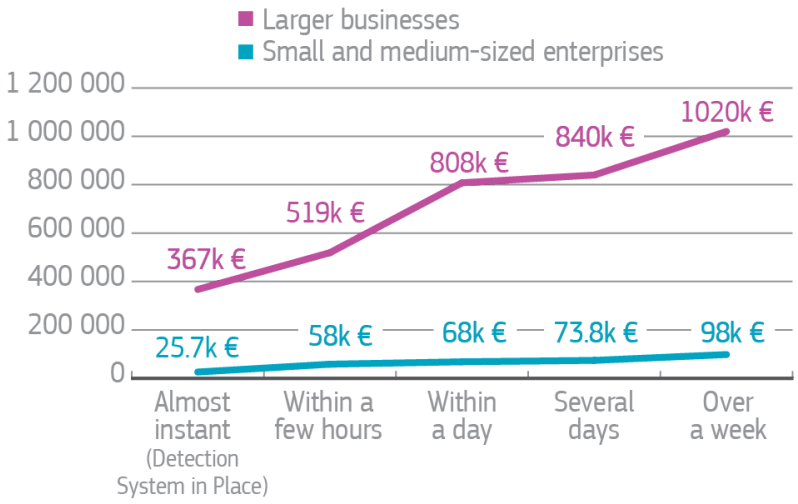

Figure 2: Increasing Costs of a Cyber Attack over time

- Studies on cyber costs point to increasing impacts to all kinds of businesses with financial services, energy, technology, services, industry and defence being the most affected sectors in 2015 but with impacts now spreading across the business world[71].
    - At the level of individual companies, various studies relating to French, German and UK-based companies have found the economic impact of cybercrime to range from €100,000/year per affected company to as much as €20m depending on the type of attack[72]. These figures are likely to increase as more and more economic infrastructures become connected[73].
    - The costs related to cybercrime and data breaches are thought to be significant and growing fast as digitalisation spreads into all spheres of our lives[74]. A 2014 study estimated the economic impact of cybercrime in the Union to stand at 0.41% of the EU GDP (i.e. around 55 billion euro) in 2013; with Germany being the most affected Member State (1.6% of GDP)[75]. Europol currently estimates the cost at 265 billion euro per year[76].

[71] Ponemon Institute, '2015 Cost of Cyber Crime Study: Global', October 2015, http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states.
[72] European Union Agency for Network and Information Security (ENISA), 'The cost of incidents affecting CIIs', August 2016, https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/.
[73] Juniper Research, op. cit. 2015.
[74] https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.
[75] McAfee & Center for Strategic and International Studies, '*Net Losses: Estimating the Global Cost of Cybercrime*', 2014, p 9, https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.
[76] Europol, European Cybercrime Centre, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime.

- The trend is set to rise. A recent study by Juniper Research forecasts that the economic cost of data breaches will quadruple by 2019, to reach 2 trillion euro worldwide[77]. Costs to critical infrastructures and businesses could escalate with fines imposed by the GDPR. Monetary penalties for breaching the UK data protection laws totalled £3.2m for 35 incidents in 2016, as one example of the costs of regulatory enforcement[78]. Cyber-attacks are set to cost businesses globally as much as $2.1tn (€1.9tn) by 2019.

- The way businesses use available budgets and resources will be vital in the coming years, in keeping the financial and reputational impact down, and in minimising losses. Training and education on cyber threats is vital to creating a savvier and less vulnerable workforce. Alongside detection technology, clued up and vigilant staff who are more informed and aware of the risks facing businesses today and tomorrow will help improve detection and minimise impact.
    - The Kaspersky study on IT security risks highlights that without the benefit of insight and intelligence, organisations will remain unable to improve detection and combat the growing number and severity of cyber threats. Only by moving beyond prevention towards recovery and mitigation will organisations be able to reduce their risk and the inevitable financial consequences of a cyber attack[79].
- Most businesses do not have a strong imperative to consider financial cost of breaches, nor do senior managers typically ask for any costings. Most businesses do not perform on-going monitoring of financial costs of cyber security breaches. This is a common practice only in 5% of the companies surveyed. Large companies, and companies operating in financial and insurance are more likely to monitor financial impacts but the number of businesses so remains low.
- Many businesses are not investing in cyber security and therefore do not think it is worth monitoring the cost of breaches, but some would like advice on better monitoring costs.
- Overall, businesses can better understand return on investment for cyber security if they can better estimate the costs of a cyber-attack or data breach and understand the ramifications for its business or operations.

4.2 Applying a business lens to risk management: Key messages for EU businesses

- Hard-earned reputations can be lost in a flash. There has never been a more important time for businesses to assess their data defences and ensure that business-critical information and sensitive data are properly secured.
- If the WannaCry and other recent attacks have taught us something, it is the validity of risk-based cyber security[80]. These recent attacks have provided several proof points that security is not simply a technology problem, but a business risk issue.
    - By targeting known vulnerabilities, WannaCry highlights the issue with people, process and technology in terms of making sure systems are patched.
    - Risk management is the recipe for mitigating risk. This means that businesses of all sizes should be creating a business-driven security strategy, which is the convergence of

[77] Juniper Research, Press Release: 'Cybercrime will cost businesses over $2 trillion by 2019', 12 May 2015, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.
[78] http://ow.ly/QCgj30cyuyh.
[79] http://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf.
[80] http://www.computerweekly.com/news/450419870/WannaCry-shows-validity-of-risk-based-security-says-RSA-head?utm_content=control&utm_medium=EM&asrc=EM_ERU_77933468&utm_campaign=20170601_ERU%20Transmission%20for%2006/01/2017%20(UserUniverse:%202383547)&utm_source=ERU&src=5639188.

security and risk management. Risk management assumes greater importance also as the GDPR approaches.

- Organisations need to take control of all risk, not just cyber risk, and have a framework, process and set of tools to support efforts in taking a risk-based approach.
- Risk management has never been more important and requires change management within organisations. Businesses need to manage risks and understand what measures they have in place to protect themselves and their customers. Insurance can play a role in helping businesses cover financial losses, meet regulatory obligations and deal with potential operational and reputational fall-outs.

4.3 Helping Businesses prepare for the GDPR and breach notifications

- The GDPR, which comes into force on 25 May 2018, will considerably strengthen the existing rules and responsibilities around how businesses process and safeguard consumer data. The GDPR enshrines fundamental privacy rights for consumers, such as "the right to be forgotten" and the right to object to profiling activities, which businesses have to comply with.
- Lloyds of London provide illuminating pointers on how businesses are preparing for the GDPR[81]. The GDPR should become a lever for all companies to adopt a risk management strategy that enables them to ensure data is adequately protected.
  - Despite the implications of the GDPR, the survey found that 57% of business leaders admit not fully understanding the potential implications of the GDPR on their company, with 12 months to go before the rules come into force.
  - 97% of respondents have heard of the GDPR but only 7% report knowing a "great deal" about it, while 64% are aware it could result in an investigation of their business and 58% aware of the financial penalties.
  - In the light of the GDPR, there is no room for complacency. Businesses also need to accelerate breach identification as hackers can roam the network undetected and cause unlimited damage. There will be a large number of organisation unaware that they have been or are being attacked at any given time.
  - The GDPR will force organisations to comply with a mandatory breach notification window, which places additional pressure on business to spot and disclose a breach within 72 hours. This necessitates a deep understanding of all activity happening across the entire network, at all times. Clearly the GDPR cannot be ignored.

    The figure below shows the extent to which business and IT leaders in 3 European countries are not yet GDPR-ready.

[81] http://www.privacyrisksadvisors.com/news/lloyd-s-survey-facing-the-cyber-risk-challenge/.

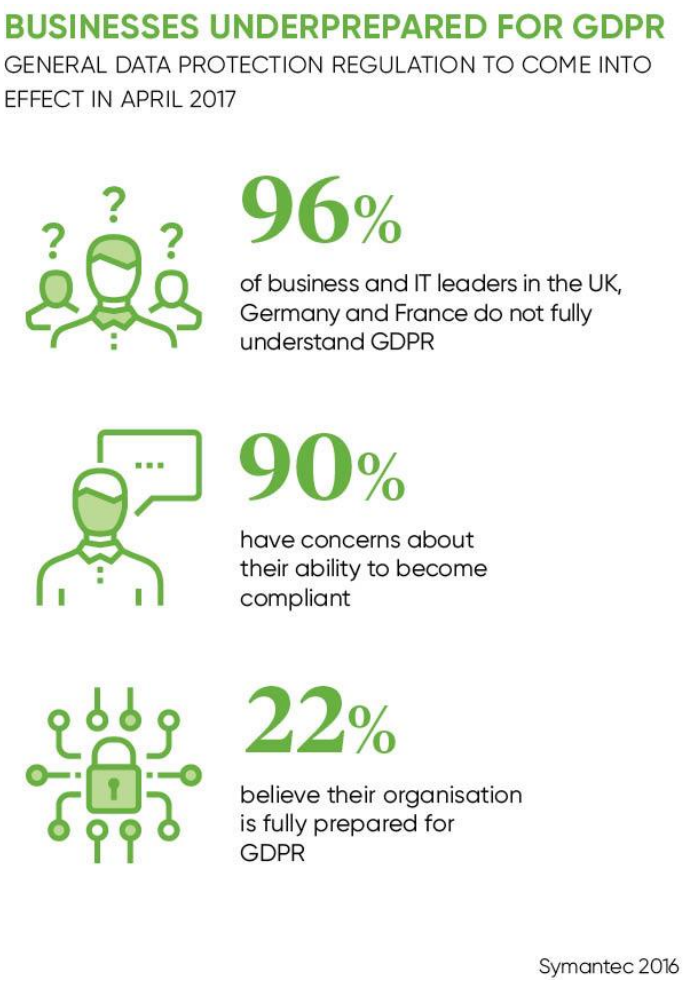

Figure 3: Business Preparedness for GDPR

- Because many companies are failing to share information on attacks and the extent of the losses incurred for fear of their reputation, it is difficult to estimate the financial cost of cyber-attacks. The LinkedIn and Yahoo breaches illustrated the vulnerability of such companies, as well as the potentially important detrimental impact on image and long-term business perspectives of such attacks.
    - Lack of reporting and information-sharing relating to cyber incidents represents a major hurdle to better understanding and addressing cyber threats and provides scope for new vulnerabilities to spread more widely. Under-reporting actually results from an unawareness of breaches and other intrusions due to a lack of detection capabilities.
    - Other factors of corporate under-reporting include reluctance of IT management teams to inform senior management; lawyers advising their clients against reporting; or those affected simply not knowing who to turn to in the event of an attack[82].
    - Under-reporting appears to be particularly prevalent in Europe, where, so far, very few large companies have publicly acknowledged a cyber breach. The entry into force of both the GDPR[83] and the national implementation of the Directive on Security of Network

[82] UK National Crime Agency: 'Cyber Crime Assessment 2016', 7 July 2016, http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.
[83] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

and Information Systems ('NIS' Directive)[84], will subject certain companies to reporting requirements and should increase public awareness.

- A practical approach to the notification of data breaches comes from the UK government through its National Cyber Security Centre, as reported in the CyberWISER Cartography on the UK[85]. The final version of the Cartography (D6.10 – Demonstrator, July 2017) will further reinforce the importance to reporting cyber incidents with more complete and up-to-date information on national competent authorities and by adding this information to the list of countries covered[86]. WISER has practical drivers for facilitating organisations affected by attacks in that it has already provided support for SOC Telefonica (Spain) by linking it to the Cyprus national CERT because they were unable to find the right contacts (in this case the information was only available in Greek).

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016/L 119/1.

[84] Directive (EU) 2016/1148.

[85] https://www.ncsc.gov.uk/incident-management. See also, https://www.cyberwiser.eu/united-kingdom-uk.

[86] https://www.cyberwiser.eu/cartography.

5 CW-SEIT Online Tool

5.1 Overview of CW-SEIT

Figure 4: CW-SEIT logo

The overriding strategic goal of CW-SEIT is to boost uptake of CyberWISER service packages by SMEs and also to support the portability to verticals other than the current pilots (financial services – insurance and energy – supply and smart grids).

Enhancements for the new CW-SEIT will simplify the approach for European digital SMEs, many of which have fewer than 15 employees, in understanding the importance of risk management and help them make it a top business priority. In this respect, it also provides guidance on the GDPR, which may further increase the financial costs of a data breach.

As a WP8 tool, its purpose is also to guide SMEs, small teams in public administration and even large businesses, on the use of the CyberWISER service packages.

It is therefore important to clarify that the tool has a distinctive value proposition compared with impact assessment offered in CWE and CWL in that CW-SEIT facilitates risk management as a first essential step towards cyber security suited for SME needs. Another important distinction is that CW-SEIT is a free, online educational tool, whereas CWE and CWP have an important market value for WISER, and are central to exploitation and the business model under WP8.

Features of CW-SEIT - Impact Assessment of cyber-attacks

- The questionnaire contains 10 key questions tailored to small business understanding of cyber risks based on similar tools designed within the consortium for the same audience.
    - 4 initial questions collecting business-related data from potential WISER leads, thus supporting portability to other verticals in WP7.
    - 1 question is designed to prompt information on different levels of understanding of the GDPR.
    - 5 questions relating to cyber risk management practices and implementation of mitigating measures, and point users to relevant CyberWISER service packages.
- A New WISER Checklist on Cyber Risk Management adopts a practical approach to cyber risk management based on 3 different phases (planning, implementing and reviewing) to encourage companies to make it a central part of business without overburdening them with too much information.
- The downloadable report provides tailored information on cyber risk management, including valuable insights on socio-economic impacts (as defined in section 1), and recommended best practices, as well as pointers to the CyberWISER service packages.
- Follow-up actions for potential leads: demo and initial consultancy requests.

Answers are mostly restricted to three options that are easy to understand and provide insightful texts. The weighting of risks, which is based on the findings reported in the previous sections, is restricted to three levels “Low”, “Medium” and “High” to ease SME understanding.

5.2 CW-SEIT Messages for EU Businesses

European businesses face a constantly evolving landscape of cyber risks.

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and applies to any company dealing with goods and services to EU citizens, or that monitors their behaviour. It also introduces a series of requirements for businesses that suffer a data breach, including having to report a cyber breach within 72 hours or face significant fines. Clearly the GDPR cannot be ignored.

Risk management is *the* recipe for mitigating risk. This means that businesses of all sizes should be creating a business-driven security strategy, which is the convergence of security and risk management. The GDPR is also a good use case, as is every threat and vulnerability, with a view to balancing the threats, opportunities and resources.

What is at risk? Your money, your information, your reputation, your IT equipment and your IT-based services. Information is an asset that can take many forms: client lists, customer databases, your financial details, your customers’ financial details, deals you are making or considering, your pricing information, product designs or manufacturing processes. There is a risk to your IT services and information wherever they are stored, whether held on your own systems and devices, or on third-party hosted systems (i.e. ‘in the cloud’).

Who could pose a threat to these assets? Current or former employees, or people you do business with: compromising your information by accident, through negligence, or with malicious intent. Criminals: out to steal from you, compromise your valuable information or disrupt your business because they don’t like what you do. Business competitors: wanting to gain an economic advantage.

What impact could an attack have? Financial losses from theft of information, financial and bank details or money. Financial losses from disruption to trading and doing business – especially if you are dependent on doing business online. The worst breaches can result in a business being put of action for up to 10 days. Losing business from bad publicity & damage to your reputation & customer base. Costs from cleaning up affected systems and getting them up and running. Costs of fines if personal data is lost or compromised. Damage to other companies that you supply or are connected to.

CW-SEIT helps businesses, especially SMEs, to understand the financial costs, tangible and intangible impacts of data breaches and guides them in managing their cyber risks.

5.3 New WISER Checklist for Cyber Risk Management

The WISER basic guide is based on a UK government guide for SMEs and comprises three parts: **Planning, Implementing and Reviewing**. Each part comes with a checklist, providing a practical approach manageable by most SMEs, however small.

Risk management is an essential part of information security. It helps businesses manage risks and understand what measures to put in place to protect their business and customers. Risk management is also essential in view of the EU GDPR, which comes into force on 25 May 2018 and is applicable to any organisation dealing with goods and services of EU citizens or that monitors their behaviour.

Part 1 - Planning

Take these steps to help make information security part of your normal business risk management procedures.

Your checklist

1. *What information assets are critical to your business?*

Do not make the common mistake of thinking your business is too small to be at risk. The assumption that small businesses, which often operate without dedicated IT professionals, and rarely regard

themselves as attractive targets for cyber-attacks with the knock-on effect of being left undefended, is precisely what makes SMEs attractive to hackers.

Consider whether your business could be a target - this will indicate the level of risk your business is exposed to.

You need to take control of all risk supported by a framework, process and set of tools to support efforts in taking a risk-based approach.

What kinds of risk could they be exposed to?

Carefully assess which of your business assets would be most damaged by a cyber-attack. Risks span your customer or even staff data, intellectual property or your partnerships with larger companies by posing a 'soft target' for hackers.

Identify the financial and information assets that are critical to your business, and the IT services you rely on, such as the ability to take payments via your website.

Assess all the IT equipment within your business, including mobile and personal IT devices. Understand the risks to all of these things by considering how they are currently managed and stored, and who has access to them.

Assess the level of password protection required to access your equipment and/or online services by your staff, third parties and customers, and whether it is enough to protect them.

Ensure that your staff have appropriate awareness training, so that everyone understands their role in keeping the business secure.

2. *What legal and compliance requirements is your business subject to?*

Risk management has never been more important and requires change management within organisations. Businesses need to manage risks and understand what measures they have in place to protect themselves and their customers. This also applies to being GDPR-ready, as a first step towards compliance. Check out our guide to new EU regulations such as the General Data Protection Regulation and the Network Information Security Directive (NISD), available in several European languages [links].

3. *How could you continue to do business if you were attacked?*

Remember that many types of breaches take weeks or months to detect; a fair number may never be detected at all. This is usually the case in SMEs and organisations that have low levels of cyber protection.

Have a back-up plan in the event of a cyber-attack resulting in a data breach. Make sure you know how to outsource the right professional support. Also make sure you have at hand contacts for local police and/or national computer response teams, usually called CERTs to report the attack and get help [link to new cartography overview from D6.10].

You may also like to consider whether cyber insurance could protect your business against any impacts resulting from a cyber attack.

4. *How can you manage these risks on an ongoing basis?*

Decide whether you need to make an investment, or seek expert advice, to get the right security controls in place for your business.

Use CyberWISER Light with its self-assessment risk profiling and vulnerability testing. This FREE online tool is designed for use also by CEOs and other non-technical personnel for a company-wide approach to cyber risk management.

You can use the CyberWISER Light Fast Track [link] *to assess your risk profile and help you define your risk management strategy even if you do not have IT professionals working in your company. This online tool collects information to determine the cyber risk exposure of your company based on your responses to the questionnaire, particularly your business profile, your company structure and set-up, and the threat exposure of the sector in which you operate. The online assessment does not require the installation of any software on your IT infrastructure.*

CyberWISER Light [link] *also features vulnerability testing, which detects cyber threats related to your business. Using it on a* regular basis *gives you fresh data on your vulnerabilities, which is essential for maximum protection. This means you can update your cyber risk management plan to reflect new threats you are exposed to.*

It is highly recommended that every small business should adopt a basic tool as a first approach to cyber risk management,

Implementing

Take these steps to put the right security controls in place for your business. If you use third-party managed IT services, check your contracts and service level agreements, and ensure that whoever handles your systems and data has these security controls in place.

Your checklist

1. *Have you put in place the right security controls to protect your equipment, information, IT system and outsourced IT services?*

***Ransomware** is more than merely a nuisance. While the infected computer can still be used, the risk of losing valuable data can impact productivity. With that in mind, there are ways to counteract or avoid a ransomware attack. The best defence is to remain vigilant. Small business owners can be especially vulnerable to ransomware attacks, as they may lack the funds to institute strong security measures. However, as long as data is kept safe and protected and users remain vigilant, ransomware can be defeated before it gains a foothold in a computer.*

***Malware protection:** install anti-virus solutions on all systems, and keep your software and web browsers up to date. Consider restricting access to inappropriate websites to lessen the risk of being exposed to malware. Create a policy governing when and how security updates should be installed.*
***Network security:** increase protection of your networks, including wireless networks, against external attacks through the use of firewalls, proxies, access lists and other measures.*
***Secure configuration:** maintain an inventory of all IT equipment and software. Identify a secure standard configuration for all existing and future IT equipment used by your business. Change any default passwords.*
***Managing user privileges:** restrict staff and third-party access to IT equipment, systems and information to the minimum required. Keep items physically secure to prevent unauthorised access.*
***Home and mobile working, including use of personal devices for work:** ensure that sensitive data is encrypted when stored or transmitted online so that data can only be accessed by authorised users.*
***Removable media:** restrict the use of removable media such as USB drives, CDs, DVDs and secure digital cards, and protect any data stored on such media to prevent data being lost and malware from being installed.*
***Monitoring:** monitor use of all equipment and IT systems, collect activity logs, and ensure that you have the capability to identify any unauthorised or malicious activity.*

Other checklist points are addresses under Planning and include:

Do your staff know what their responsibilities are? Do they know what good practices look like?
If you are attacked or something goes wrong, how will you deal with it and get back to business?
Who will you turn to for help?

WISER can help you connect all your IT to the risks you face and help you prioritise them even if they have limited resources. It can also help them align better on business and technical goals, by defining a company-based cyber strategy using the tools they need to assess risks and communicate effectively.

CyberWISER Essential comprises services that can be packaged to meet your specific business needs.

*The **self-assessment questionnaire** collects inputs on the business profile, the ICT profile, and infrastructure elements to allow the services to create a more complex and elaborate correlation between IT- and business-related risks.*

Vulnerability testing*: broad range of vulnerability scanners enables the detection of a wider range of vulnerabilities compared with CWL.*

DSS societal impact evaluation*: features a list of basic mitigation measures based on international best practices & WISER experience. On top of that, the societal impact of the risk is analysed, offering a dimension of the risk, which is real but not evident, and has a clear potential impact on the company business.*

Real-time monitoring*: A Security Information and Event Management (SIEM) solution and a correlation engine that continuously analyses security events, aggregating data from many sources. Combined and correlated data generates reports and alerts.*

Real-time risk assessment*: based on the analysis of information about the company configuration and its ICT profile, provided via a questionnaire during the configuration steps, events and alarms coming from the target infrastructure monitoring module and vulnerabilities detected by the monitoring scanners. On top of that, the societal impact of the risk is also analysed.*

Risk Modelling system: *a widget of a risk model library, enabling the user to download, change and upload a new risk model relevant to the company.*

WISER sensors and agents *are installed in the IT infrastructure to detect potentially harmful events and vulnerabilities. The customer installs the sensors and agents using the WISER guidelines, with WISER consultants available for additional help if needed. The sensors cover only the network layer and basic sensor management functionality.*

Dashboard*: reports high-level charts and diagrams which provide valuable at-a-glance information about sensor variables and incidents detected by the monitoring infrastructure. Professionals without IT security expertise can use it to make informed decisions based on the information available.*

Online service support*: WISER team of consultants with considerable expertise on cyber security and specific knowledge about the WISER Framework.*

Reviewing

Take these steps to review your security and respond to any changes or problems you identify, including attacks or disruption to business.

Your checklist

1. *Are you reviewing and testing the effectiveness of your controls?*

Test, monitor and improve your security controls on a regular basis to manage any change in the level of risk to your IT equipment, services and information.

Remove any software or equipment that you no longer need, ensuring that no sensitive information is stored on it when disposed of. Review and manage any change in user access, such as the creation of accounts when staff arrive and deletion of accounts when they leave.

If your business is disrupted or attacked, ensure that the response includes removing any ongoing threat such as malware, understanding the cause of the incident and, if appropriate, addressing any gaps in your security that have been identified following the incident.

Remember that if you fall victim to online fraud or attack, you should report the incident to the competent authority. [Link to CyberWISER Cartography].

From 25 May 2018, under the GDPR, you will need to make the notification within 72 hours. You may also need to notify your customers and suppliers if their data has been compromised or lost. Decide on the best way to do this.

Other things to consider are:

Are you monitoring and acting on the information you receive?
Do you know what the latest threats are?

CyberWISER Plus provides a complete framework, processes and services necessary to make your company cyber-secure even in today's fast-evolving landscape, including cost-benefits that will help you make informed decisions about investments on cyber products, services and insurance.
The services can be packaged to meet your specific business needs.

***The self-assessment questionnaire** collects inputs on the business profile, the ICT profile, and infrastructure elements to allow the services to create a more complex and elaborate correlation between IT- and business-related risks.*

***Vulnerability testing**: broader range of vulnerability scanners enables the detection of a wider range of vulnerabilities compared with CWL.*

***DSS societal impact evaluation**: ranks and prioritises the mitigation measures based on societal or indirect impacts (defined in D8.3 as tangible and intangible). As the societal impact is closely related to reputational damage (intangible), which, can have a very negative effect on the company's finances [see Case Studies on Talk Talk and Yahoo!, to be extracted from sections 2.2.1 and 2.2.4]. This WISER feature contributes to raising awareness about one of the aspects of the cyber risk that is usually neglected, and which is stressed in CW-SEIT.*

***Real-time monitoring**: A Security Information and Event Management (SIEM) solution and a correlation engine that continuously analyses security events, aggregating data from many sources. Combined and correlated data generates reports and alerts.*

***Real-time risk assessment**: high degree of customisation and wide range of inputs as the information available has both high quantity and quality and the models used are more complex. In addition, it features a cost-benefit analysis of the mitigation measures generated by the Risk Assessment Engine.*

***Risk Modelling system:** a widget of a risk model library, enabling the user to download, change and upload a new risk model relevant to the company.*

***Sensor installation**: WISER sensors and agents are installed in the IT infrastructure to detect potentially harmful events and vulnerabilities. The customer installs the sensors and agents using the WISER guidelines, with WISER consultants available for additional help if needed. Sensors cover both the network layer and the application layer. In CyberWISER Plus the scope of the sensors covers not only the network layer, but also the application layer. The monitoring and testing techniques produce high-quantity and high-quality data collected from the target infrastructure. It also enables location of customised sensors tailored to the specific nature of the target infrastructure and integrates existing sensors provided to the customer, which requires the involvement of the WISER team.*

***Dashboard**: reports high-level charts and diagrams which provide valuable at-a-glance information about sensor variables and incidents detected by the monitoring infrastructure. Professionals without IT security expertise can use it to make informed decisions based on the information available.*

***Cost-benefit analysis**: The main advantage of cost-benefit analysis is that companies can rank and prioritise measures based on the rates provided. CyberWISER Plus represents a novelty for senior management which usually lacks this information, preventing informed decisions that are gaining in importance. In practice, it means that managers no longer need to put their trust in other criteria or implement measures with reduced scope but that require big investments. CyberWISER Plus helps you steer the company security policy.*

***Online service support**: WISER team of consultants with considerable expertise on cyber security and specific knowledge about the WISER Framework, combinable with onsite support.*

***Onsite service support**: Providing an extra layer of advanced support for specialised set up and tailored configuration.*

5.4 The new CW-SEIT Questionnaire

The table below represents a revised version of CW-SEIT questionnaire taking into consideration the main findings of the updated analysis. Questions are tailored to SME characteristics such as low number of personnel and small (if any) IT teams.

ID	Question	WISER motivation

1	What business sector do you operate in?
	• *Agriculture, including fisheries*
	• *Automotive*
	• *Construction*
	• *Energy and Power*
	• *Entertainment and the Arts*
	• *Finance and insurance*
	  ○ *Bank*
	  ○ *Fintech*
	  ○ *Insurance*
	• *Healthcare*
	  ○ *Hospital or healthcare facility*
	  ○ *Medical devices*
	• *Information and Communications Technologies (ICT)*
	• *Manufacturing*
	• *Public administration*
	• *Real estate, rental and hiring*
	• *Retail trade*
	• *Transportation and warehousing*
	• *Wholesale trade*
		User information and mapping of high risk sectors. Gathering data also in relation to portability to other verticals (WP7)

2	How big is your company? • *1-5 employees* • *6-20 employees* • *20-50 employees* • *50-150 employees* • *150-250 employees* • *More than 250 employees*	Customer information gathering plus intelligence on ability to define a risk management strategy, as well as ability to detect an attack and respond to it depending on human resources (WP7).
3	What is your company's annual turnover? • *EURO 0-1 Million* • *EURO 2-5 Million* • *EURO 5-50 Million* • *EURO 50-500 Million* • *EURO 500 Million to 1 Billion* • *Above EURO 1 Billion*	Customer information gathering with specific reference to ability to pay for cyber risk management services and products (WP7)
4	In what country are you based? *List of EU member countries + CH, ISL, NO and UK in alphabetical order*	Customer information gathering. Gauging current trends and expected risks (WP7)
5	Has your company ever suffered a cyber-attack? *Yes* *No*	Concise WISER Guide on threats and evolving landscape.

	Don't know	
6	How well would you describe your understanding of the General Data Protection Regulation (GDPR)? *Low (little or no understanding)* *Average (understanding of some aspects)* *High (full understanding)*	Concise WISER Guide on the GDPR, highlighting the importance of risk management
7	Does your company use self-assessment cyber risk assessment tools on a regular basis? *Yes* *No* *Don't know*	WISER checklist part 1 (planning) up to CWL Fast Track[87]..
8	Does your company regularly carry out vulnerability testing to identify cyber risks it could be facing? *Yes* *No* *Don't know*	WISER checklist part 1 (planning) including part on CWL.
9	Which of the following cyber security measures do you already have in your IT system? • *Sensors and agents installed in your IT infrastructure to detect potentially harmful events and vulnerabilities.* • *Real-time monitoring for rapid vulnerability detection.* • *Real-time risk management for implementing swift responses to detected vulnerabilities.* • *None of the above.*	WISER checklist part 2 (implementing) including CWE service packages.
10	Which of the following cyber risk management practices have you already implemented? • Cost-benefit analysis to compare and rank different measures that could implemented. • Risk Modelling for both quantitative and qualitative risk models. • Risk Analytics for more detailed information on each risk and the current overall risk status. • None of the above	WISER checklist part 3 (reviewing) including CWE service packages.
Next Steps: Download your tailored report. Request a Demo [email + organisation] Request an initial consultation [email + organisation]		

Table 5: New CW-SEIT Questionnaire

5.5 Sample of results generated

The tables below provide an overview of the kind of information CW-SEIT V2.0 will generate based on responses provided. We show information generated for data gathering exercises, guides on risk management, on becoming GDPR-ready, the WISER checklist (parts 1,2,3) and pointers on the service packages.

Q	Results
1-4	For questions 1 – 4, text is generated **only** in cases where cyber risks are expected to be

[87] Related WISER service refers to the relevant service described in D2.6, section 2.2.

high to very high according to WISER findings. This approach is aligned with other popular online tools designed for SMEs, such as CloudScout[88], where the initial set of questions are about the SME respondent as an information-gathering exercise. The main difference being that WISER uses responses to identify potential leads and provide insights and best-practice advice in some specific cases.

A brief explanation is given below of the cases in which text is generated by CW-SEIT:

As a rule of thumb, responses generate text only for high-level risks identified by WISER.

Q1 Sector: Text is generated for respondents operating in one of the following sectors: financial institutions and FinTech firms, healthcare and medical devices, energy and power. These are considered to be high risk/reward according to the findings from the WISER analysis on the cyber threat landscape (Sections 2-4): An example for FinTech is provided in Table 7 below.

Q2 Company size: Text is generated in cases where organisation size is expected to have a significant risk with regard to the ability to detect, deter and deal with a cyber-attack, and particularly if they operate in one the above high risk/reward sectors. In this case, a successful attack could life-threatening for the business.

Given that most very small businesses are very common in Europe, CW-SEIT will increase the score for companies with up to 50 employees (an attack could have critical consequences, not only financially but also in terms of reputational damage).

Q3 Annual turnover.
For high revenue companies, the text generated focuses on the strategic advantages of conducting a cost-benefit analysis:
When it comes to putting in place appropriate countermeasures to cyber threats and successful attacks, most companies do not properly understand the extent of a potential cyber breach, both in terms of direct and indirect impacts.
The CW-SEIT provides a first step to cost-benefit analysis helping you to make more informed decisions about investments in cyber security products, services, and cyber insurance. This tool provides a template to help you determine:
The total costs (investment + maintenance).
The total future benefits.
The investment margin (benefits – costs).
The ROSI (Return of Security Investment): (benefits – costs) / costs. The mitigation measure with a positive ROSI is worth applying. The measure with the highest ROSI provides maximum value for money.
If your company is high risk/reward and you have sufficient budget, you may consider using the CyberWISER Plus service package, which includes a more advanced cost-benefit analysis. More details are provided in your FREE downloadable report, tailored to your specific case.
Cost-benefit estimations is a complex area. If you need a deeper understanding of cost-benefit calculations, please refer to our online list of resources: www.cyberwiser.eu/cw-seit-resources.
Q4 Country: CW-SEIT generates text that draws on data from Lloyds of London. According to this report, countries in northern and central Europe have a high record of data breaches. Therefore, countries in these regions will be scored higher than in other regions.

Indication of Q1-4 high scores
SME Respondent: *FinTech – 16-20 employees - EURO 5-50 Million – Sweden*. Score would be high to very high-risk exposure with texts on 1) Fintech risk landscape (Table 7) and 2) text for Q3 indicated above.

[88] http://cloudscout.cloudwatchhub.eu/#/app/home?lang=en&code=en, which has been used over 1200 in the last 12 months alone.

Q	Results
5	Answer: "Yes" all business sizes. *The complex and fast-evolving cyber risk landscape is broadening the potential for damage across organisations of all types and sizes. Recent attacks have generally caused more extensive damage and higher impacts. It is vital to remain vigilant and implement a risk management strategy.* *You should also be aware that some types of malware are now publicly available, significantly lowering technical barriers to launching large and sustained Distributed Denial of Service (DDoS) attacks, which, at the very least, will cause the interruption of your online service. This can be costly in terms of lost business due to an outage (economic impact) but also damage to reputation (societal impact).* *While DDoS attacks have been around for some time, they now tend to last longer, which increases the potential for damage, including financial costs that can increase considerably the longer they remain undetected or unresolved.* *You should also be aware that the consequences of an attack may not always be short term. Some impacts depend on success phishing or fraud attempts in the months following an attack.* *So, whether the attack was recent or not, your business assets could still be at risk.*
5	Answer: "No" and "Don't know" for businesses with 1-50 employees (text in italics indicates the text that only appears in the online form) *Small businesses often believe that they are too small to become a victim of a cyber attack. In reality, many successful attacks against small firms on a daily basis. For example, attacks on UK businesses reached 1000/day between November and December 2016, double the number of attacks since 2015 and reaching 230,000 cyber-attacks on UK SME.* *SMEs are just as interesting for cybercriminals as large companies, and can become common targets because of the data they hold. Hackers take advantage of small businesses having lower defences than larger organisations, usually due to lack of financial and human resources.* *If your website is your main sales channel, then it is a critical asset for your business. Your website could be attacked to obtain financial information, such as credit card details, from your customers, usually because it is easier to attack than those of big organisations.* *If your business is innovative and niche, you are very attractive to the bad guys on the web interested in your intellectual property and customer data. Cybercriminals know exactly how to pick the weak targets.* *If your business is connected to a larger business partner (e.g. as a supplier), you are also at risk as a "soft target". As a "soft target, cybercriminals could exploit your online weaknesses to gain access to your business partners, which might otherwise be harder to target.* *It is also important to note that*
Q	**Results**
6	Answer: "High (full understanding") – basic reminder of the financial implications and also possible intangible (socio) impacts such as damaged reputation and erosion of trust. More complete answer for *"Low (little or no understanding)" and "Average (understanding of some aspects)"* – any type of sector, company size and country. *The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 to considerably strengthen the existing rules and responsibilities around how businesses process and safeguard consumer data. It is important to note that the GDPR applies to any company that deals with goods and services to EU citizens or that monitors their behaviour. In the light of the GDPR, there is no room for complacence.* *Costs to critical infrastructures and businesses could escalate with fines imposed by the GDPR. As an example, monetary penalties for breaching the UK data protection laws totalled €3m for 35 incidents in 2016, considerably more than in previous years.* *Cyber risk management is key for ensuring your organisation is GDPR-ready. You should use the GDPR to start improving your cyber security strategy practices. Make sure everyone in the company understands the implications by providing dedicated training on the new regulation. Our advice is for everyone in the organisation to take responsibility for ensuring*

	data is adequately protected, identifying your risk tolerance, understanding how well developed your defences are, and defining a strategy to prioritise your most important business assets. *Large organisations can usually afford to hire a Chief Information Security Officer (CISO) or Chief Risk Officer (CRO). In this case, it is important that the CISO and/CRO acts as a bridge between the board and the IT department as it is very paramount to engage at this level.* *Smaller organisations who cannot afford to hire a CISO or CRO, can set up a Security Work Group or appoint a Champion within the organisation responsible for its Cyber Risk strategy.* *It is also important to note that the GDPR will force organisations to comply with a mandatory breach notification window, which places additional pressure to spot and disclose a breach within 72 hours. This necessitates a deep understanding of all activity happening across the entire network at all times.* *WISER best practice recommendations: Businesses of all sizes need coherent advice on real and focused business risks. Addressing the EU GDPR now will allow businesses to budget and prepare, by taking manageable measures to help protect the organisation from the potential fallout of non-compliancy.* *In case of data breach, use the WISER cartography* [link] *to find competent authorities in your country to whom the breach must be communicated.*
Q	**Results**
7	Answer: "No" and "Don't know" Generates the text from the WISER Checklist 1 up to and including the reference to CWL – Fast Track. Answer: "Yes" Generates texts only on CWL-Fast Track and CWL.
Q	**Results**
8	Answer: "No" and "Don't know" Generates the text from the WISER Checklist 1 up to and including the reference to CWL. Answer: "Yes" Generates texts only on CWL.
Q	**Results**
9	Answer: "No" and "Don't know" Generates the text from the WISER Checklist 2 up to and including the reference to CWE. Answer: "Yes" Generates texts only on CWE.
Q	**Results**
10	Answer: "No" and "Don't know" Generates the text from the WISER Checklist 3 up to and including the reference to CWP. Answer: "Yes" Generates texts only on CWP.

Table 6: Sample of Results Generated

Sample texts on high-risk sectors	
Q1	If respondent clicks on FinTech, the following text appears before the WISER Checklist *As a FinTech, you have important innovations the intellectual property of which needs guarding from cybercriminals. You may also hold important financial, market and customer data. Not protecting your business from cyber risks could damage it in several ways, such as theft of intellectual property and valuable data. Your hard-earned reputation can be lost very quickly. A cyber-attack could also reduce new business opportunities such as partnerships with larger financial institutions.* The Hyperfinance Report (April 2017) highlights that *71% of established institutions see cyber security as an associated risk in partnering with FinTech firms. Most large financial services firms believe better visibility of cyber security controls within FinTechs*

	would improve prospects of partnering with them. *There are many incentives for improving your cyber security.* *It is therefore very important to remain vigilant at all times as there is no such thing as a 100% secure environment. Include a strong security policy in your infrastructure as soon as you possibly can (preferably at company set-up) so it does not become a major problem later on. Understand your attack surface through vulnerability assessment as a best practice so you know what attackers might be targeting.* *Be careful about how you place user data on the Internet, especially cloud providers as lapse security configurations would allow an attacker to simply walk in and exfiltrate sensitive information.*

Table 7: Sample of texts generated for high-risk sectors

5.6 CW-SEIT Cost-benefit Analysis and Template

When it comes to putting in place appropriate countermeasures to cyber threats and actual cyber incidents, most companies fail to adequately understand the extent of a potential cyber breach, both in terms of direct and indirect impacts. There are several reasons for this:

- Cyber security is generally considered to be a technical problem rather than a business performance issue or as a good business practice based on a risk-assessment approach. Typically, staff culture does not emphasise customer confidentiality and good data management.
- Lack of key individuals in the organisation, particularly company boards, helping to champion cyber risk assessments and possible cyber insurance measures.
- Small firms are less likely to seek advice on cyber security practices, and according to the UK Cyber Security Strategy 2016-2021, have not yet started to use tools and services available to a sufficient extent despite greater awareness and high-profile media coverage.
- Most businesses do not have sufficient knowledge of the direct economic impacts of cyber risks nor of the indirect impacts due to risk exposure. Hence specific measures are not taken to mitigate such risks.

As a result, there is no support for the decision-making and the company´s managers end up taking decisions that have impact just in the short term, without any kind of underlying rationale justifying such a decision.

Part of the WISER mission is to 1) increase awareness and promote actions to mitigate risks amongst the EU business community and 2) provide a dedicated tool that is usable and useful especially to small organisations (e.g. SMEs and small IT teams in public administration) lacking the skills and means for efficient risk management but facing a variety of potential impacts. By enabling the identification of risk levels, CW-SEIT helps high risk/reward organisations to make informed decisions about investments in cyber security products and services, for example, a high value FinTech firm, whose exit strategy could be compromised by a cyber-attack.

From a technical perspective, WISER addresses these challenges by incorporating a generic methodology in order to 1) propose mitigation measures addressed to specific cyber incidents and tailored to specific infrastructure elements; 2) analyse the convenience of applying it in the light of the costs and the benefits of the actual implementation. The former is being addressed in the context of modelling (WP3) and Decision Support (WP5) activities. For the latter, this analysis serves two purposes: analyse the candidate countermeasure and, especially, compare it to other candidates. The cyber security budget is limited and the managers are interested in ensuring the maximum effectiveness of the countermeasure, thus an efficient cost benefit analysis helps companies, especially SMEs, to draw their own cyber security strategy.

WISER is a market-driven initiative, encouraging organisations to take a core set of steps towards better cyber risk management that effectively democratises cyber security (along the theme of “Cyber

Security for All"). Customised reports generated by WISER SME tools, e.g. CyberWISER Light and the CW-SEIT, gives organisations the information they need to make informed decision on cyber risk management.

WISER's innovative proposal in this respect encourages companies to establish a new culture where cyber security decisions are made in an informed manner and after a deep analysis. This makes it possible to produce an outcome understandable from the managerial and business perspective, where the costs are broken down into relevant sections and the benefits are estimated.

While the calculation of costs, despite being estimations, can be done in a systematic way with a high degree of objectivity – to a certain extent based on the state of the art in cost estimation[89], it is important to acknowledge that the estimation of the benefits is rather subjective. Historically, the financial benefits of cyber technology implementation have not been calculated with the same financial discipline used to evaluate other material investments. This is mainly due to a lack of readily available data and systematic methodology to support the efficacy of cyber investments. This gap has prevented managers from being able to formulate generally accepted financial metrics such as return of investment (ROI), net present value (NPV) and breakeven period, to communicate the value of cyber security projects and defend spending decisions[90]. In marketing literature, the concept of customer-perceived value (CPV) is used to emphasise the importance of customer´s perceptions on value[91]. Analogously, 'perceived value' can be used in security to emphasise the decision-makers perspectives.

Such value can be seen as the reduction of the risk compared with a scenario where no mitigation measures are in place. This is the intangible benefit, since investing on security measures is about avoiding risks, not about generating revenues. While there may be a general consensus on this definition, what seems really challenging is getting companies to agree upon a standard technique for calculating the internal cost of an incident. More recent discussions on security have emphasised that in the new threat landscape, security must sometimes be put before convenience and that more education in this direction is needed[92].

With a focus on bringing some extra added value to the cost-benefit analysis tool, based on Table 8 below, WISER carries out research on methods that help to ease the calculation of the benefits. A paper by Le Minh Sang Tran et al. focuses on the likelihood and consequence of the risk being diminished as result of applying one or more mitigation measures[93]. The paper also defines the thresholds of the levels of likelihood and consequence considered acceptable by the company, and selects the lowest cost combination of measures among those ensuring that likelihood and consequence levels are under the desired threshold. In a public paper[94], ENISA proposes a method to calculate Return of Security Investment (ROSI) based on 3 variables: the estimated potential loss, estimated risk mitigation, and cost of the solution. A paper by Wes Sonnenreich[95] also mentions these variables and gives some hints on how to quantify them: measure the loss on intellectual property or the loss of productivity due to a downtime. The paper also mentions that it is also important to consider what may be the impact of the measure on productivity. The advice of the author is to focus on problems that are happening every day, issues such as email spam, bandwidth inefficiency, popup ads, installation of security patches etc. rather than on major incidents less likely to happen. Another

[89] Matthias Brecht and Thomas Nowey, "A Closer Look at Information Security Costs," Working paper 2012.
[90] Allen, Hamilton Booz, "Cyber ROI: A practical approach to quantifying the financial benefits of cybersecurity," *Innovate Forward*, 2015.
[91] C. Grönroos, *Service Management and Marketing. Customer Management in Service Competition (3rd edition)*.: Haddington: John Wiley & Sons, 2007.
[92] ETSI 5G Summit, 2017, http://www.etsi.org/news-events/videos/5g-summit-etsi.
[93] Bjornar Solhaug, Ketil Stolen Le Minh Sang Tran, "An Approach to Select Cost-Effective Risk Countermeasures," *International Federation for Information Processing*, 2013.
[94] ENISA, "Introduction to Return on Security Investment: Helping CERTs assessing the cost of (lack of) security," December 2012.
[95] Wes Sonnenreich, "Return on Investment (ROSI): a Practical Quantitative Model," *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, January 2006.

example can be found in the paper by Aora et al.[96], which provides a very illustrative example based on the scenario where an organisation has to evaluate several components of its IT system in light of shrinking yearly operational budget. A very famous work that, despite being more than ten years old and which still generates a lot of discussions, is by Gordon and Loeb. The dissertation is complex with advanced maths being involved, nevertheless it is worthwhile remarking the main finding that optimal expenditures do not always increase with the increase in vulnerability, and expenditures on security should almost never exceed 37% of potential loss[97]. Other techniques, like Monte-Carlo simulations, are proposed with a special focus on the banking sector[98].

These examples show that there are several attempts aiming at defining a more rigorous estimation of the benefits of investing on a certain security measure. As research goes on, some will be shown to be more accurate than others, but a unique, universal, accurate and efficient methodology is unlikely to yield these figures. What is actually paramount, is the ability to be correct when identifying independent and measurable factors, which are very relevant for the calculations to be done, and have a deep impact on the outcome. In other words, consensus should be reached concerning: 1) the definition of 'benefit of a mitigation measure' and 2) the identification of the parameters to be used to estimate such benefit. If these two objectives are achieved, the methodology to be used is a matter of choice and experimentation.

As part of the CW-SEIT tool, WISER will make available a template that can be filled out by the user to estimate the costs and the benefits of implementing certain mitigation measures. This service will be offered for free as a teaser of what is provided in CyberWISER Plus. The CyberWISER Plus service package features a more detailed template (WISER D5.2[99]), with support provided by WISER experts. The user will be able to play with the template and compare two different mitigation measures. To help the user, the WISER website will include, in the section devoted to CW-SEIT, relevant links to bibliography ("Further Reading" – recommended for an in-depth understanding of complex calculations of costs and benefits). Once thoroughly analysed, this can enlighten the user in making a good estimation of the cost and benefits of the analysed mitigation proposals.

Cost-benefit template, guide and plans
The template used for the cost-benefit analysis has three parts and is showed in the table below. The user will be able to compare 2 mitigation measures.

1) **Investment costs:** the initial investment that has to be made to put in place the corresponding mitigation measure.
    a. **Management personnel** costs incurred by making the mitigation measure available (managerial positions).
    b. **Tech personnel** costs incurred by making the mitigation measure available (technical positions if existing within the organisation; otherwise they are managerial).
    c. **Equipment purchase** costs related to acquiring the necessary equipment to apply the mitigation measure, if any.
    d. **Software purchase** costs of acquiring any software needed to run the mitigation measure, if any.
2) **Future costs:** helps the user reflect on the cost incurred by keeping the mitigation measure available for a certain timeframe.
    a. **Management personnel** costs for managerial positions for the defined timeframe.

[96] Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang Ashish Arora, "An ounce of prevention vs. a pound of cure: how can we measure the value of IT Security solutions?," Berkeley, California. UNT Digital Library.
[97] Lawrence A. Gordon and Martin P.Loeb, "The Economics of Information Security Investment.," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457, November 2002.
[98] James R. Conrad, "Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations," in *IEEE Workshop on the Economics of Information Security*, 2005.
[99] WISER Consortium, "D5.2 - WISER Real-time assessment infrastructure," Deliverable 2016.

b. **Tech personnel** costs related for the technical profiles for the defined timeframe, which could include outsourcing. c. **Equipment updates** costs incurred by keeping the equipment up to date, in order to apply correctly the mitigation measure. d. **Software updates** costs incurred to keep the software up to date, in order to apply correctly the mitigation measure.
3) **Future benefits:** estimated benefits, for a certain timeframe, of applying the mitigation measure. a. **Reduction of damages**. The user is asked to estimate to what extent, in terms of money, the damage to company digital assets will be reduced as a consequence of applying the measure. b. **Reduction of operational costs / resources**. A data breach leads to extra expenditure on operational costs and resources to fix the problem. A clear benefit of putting in place a mitigation measure to reduce the likelihood of a cyber-attack would be to reduce these potential costs. c. **Reduction of insurance fees**. If the company has contracted an insurance for cyber incidents and attacks/data breaches occur, it is expected that the insurance premium becomes more expensive for the company. Preventing cyber incidents means keeping the insurance premium at its original level or even lowering it. This can be seen as a clear future benefit.

Table 8: Cost-Benefit Analysis Template

The result of the analysis will be a comparison of:

- The total costs (investment + maintenance).
- The total future benefits.
- The investment margin (benefits – costs).
- The ROSI (Return of Security Investment): (benefits – costs) / costs. The mitigation measure with a positive ROSI is worth applying. The measure with the highest ROSI provides maximum value for money.

CW-SEIT provides the template presented above for the cost-benefit analysis. Given the complexity of obtaining the figures with which fill the template, some relevant bibliographic entries will be linked. The user will be encouraged to read this documentation in order to define his own approach to fill the template. Additional research efforts will be made in the coming months to expand this library of resources oriented to enlighten the user in the process of establishing a framework for the decision-making process.

6 CW-SEIT Positioning and Timeline for 6-month WISER Sprint

6.1 WISER Positioning

In this section, we position the CW-SEIT tool in relation to the CyberWISER service packages as defined in D2.6 but presented here through a business lens in line with the WP8 Go-to-Market strategy. The positioning covers CyberWISER Light – Fast Track (Self-assessment); CyberWISER Light; CyberWISER Essential and CyberWISER Plus.
The related promotional packages cater to different audiences, where the postcards (*see D8.6*) can be packaged for different stakeholders in a “mix-and-match” fashion.

.

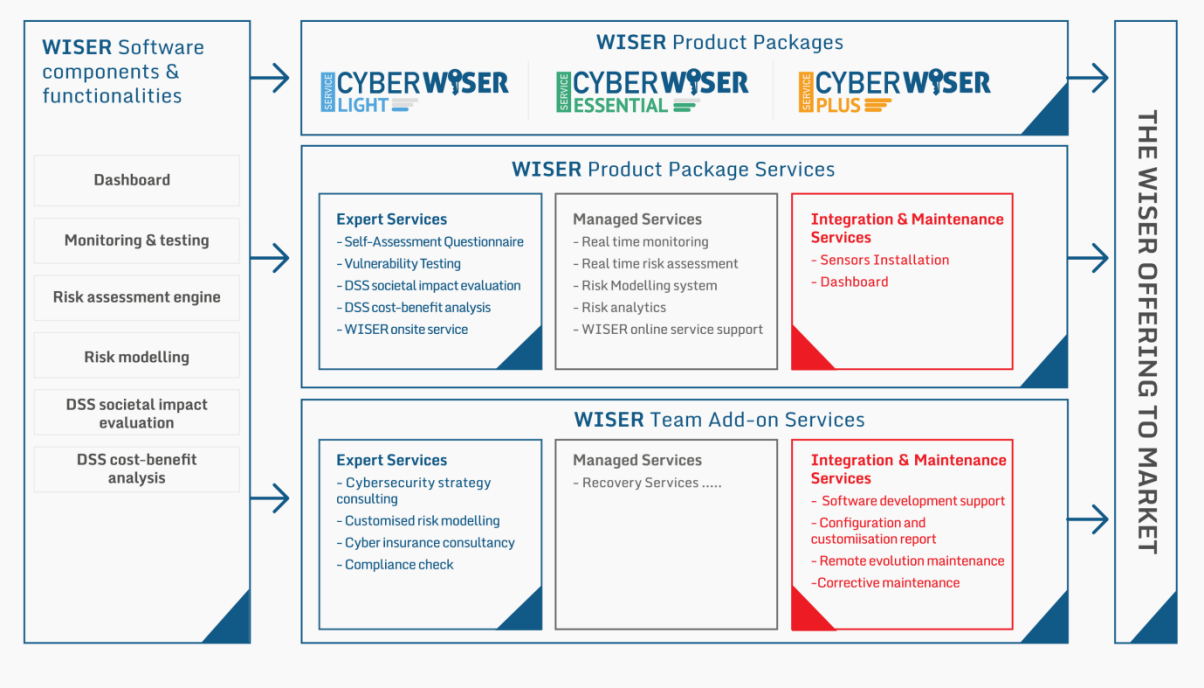

Figure 5: WISER Service Packages

CW-SEIT and CyberWISER Light are both offered for free as teasers for the core set of service packages by getting a first touch-point with customers.
An important distinction with respect to CWE and CWP is that CW-SEIT provides informative guidance on cyber risks and management practices but strategically points to the former services as part of its marketing mission underpinning the exploitation objectives.
The main purpose of CW-SEIT is to:

- Help SMEs understand the impacts of a cyber-attack from a socio-economic perspective (financial losses, tangible and intangible impacts).
- Encourage SMEs in making cyber risk management a top business priority.
- Enable SMEs to start assessing their threat surface.
- Foster uptake of CyberWISER service packages, increasing uptake and supporting portability to other verticals.
- Provide a teaser for the CyberWISER cost-benefit analysis with a dedicated template and short WISER Guide on completing it.

It is also important to note several key differences with regard to the CyberWISER cost-benefit analysis. In the more advanced service packages, for which customers will pay, the cost-benefit analysis is based on an innovative and systematic approach to compare, rank and prioritise mitigation measures. The template enables customers to estimate initial and future costs, as well as future benefits of applying a particular mitigation measure. While the costs are broken down into several parts by default, customers can customise the template by adding or removing fields. Customers can also choose the timeline along which the analysis should be performed, set a discount rate, select the currency and add constraints[100].

[100] On the development and features of the CyberWISER cost-benefit analysis, see D5.1 Section 5.3 and D5.2, Section 5.1.3.

6.1.1 CyberWISER Light – Fast-track and CyberWISER Light (FREE)

In this section, we draw on the positioning of WISER in D2.6, Section 2.

The **self-assessment questionnaire** is offered in all 3 WISER cyber risk monitoring services. The basic features available in both versions of CWL, which collects information to determine the cyber risk exposure of the respondent organisation based on inputs relating to the business profile, the internal organisation and threat exposure of the sector in which it operates.

The **vulnerability testing** in CWL detects vulnerabilities identified in OWASP top ten cyber threats, detectable with automated scanners.

It is important to note that CW-SEIT also considers other risks in an evolving landscape, placing emphasis on the importance of risk management.

Risk assessment in this context is based on the outcomes of the business and ICT profile, the business value of infrastructure elements and results from vulnerability scanners. The correlated inputs offer a cyber risk assessment tailored to management positions and enable decision-making.

Promotional message for CyberWISER Light

Who: Specially designed for small businesses and small IT teams in public administrations to help them identify and manage their risks. Users do not need to be an IT expert or risk manager to use CyberWISER Light. The tool can be used by CEOs and other non-technical members of staff for a company-wide approach.

Why: Using CyberWISER Light on a regular basis helps you update your cyber risk profile and gives you fresh data on your vulnerabilities, which is essential for maximum protection.

What: An online self-assessment tool that is FREE to use. It has two parts.

CWL Fast Track is an online self-assessment giving vital information about the organisation's risk profile. It collects general company information important for assessing potential impacts and more specific information related to cyber risk exposure. Users then download their FREE report and can use it to define mitigation actions, and should do this on a regular basis.

CWL is both an online self-assessment and a vulnerability test. The vulnerability test helps organisations prevent attacks before they happen. The test helps identify common online threats that represent serious vulnerabilities in your IT system. To take the test, you need to insert a token on the root of your server. To do this, you need to make sure or your IT manager has the right credentials before starting.

Use your FREE report to define mitigation actions, which may be actions like software upgrades or patching.

6.1.2 CyberWISER Essential – Cyber Threat Detection and Monitoring in real time

In this section, we draw on the positioning of WISER in D2.6, Section 2.

The **self-assessment questionnaire** collects inputs on the business profile, the ICT profile, and infrastructure elements to allow the services to create a more complex and elaborate correlation between IT- and business-related risks.

Vulnerability testing: broader range of vulnerability scanners enables the detection of a wider range of vulnerabilities compared with CWL.

DSS societal impact evaluation: features a list of basic mitigation measures based on international best practices & WISER experience. On top of that, the societal impact of the risk is analysed, offering a dimension of the risk, which is real but not evident, and has a clear potential impact on the company business.

Real-time monitoring: A Security Information and Event Management (SIEM) solution and a

correlation engine that continuously analyses security events, aggregating data from many sources. Combined and correlated data generates reports and alerts.

Real-time risk assessment: based on the analysis of information about the company configuration and its ICT profile, provided via a questionnaire during the configuration steps, events and alarms coming from the target infrastructure monitoring module and vulnerabilities detected by the monitoring scanners. On top of that, the societal impact of the risk is also analysed.

Risk Modelling system: a widget of a risk model library, enabling the user to download, change and upload a new risk model relevant to the company.

WISER sensors and agents are installed in the IT infrastructure to detect potentially harmful events and vulnerabilities. The customer installs the sensors and agents using the WISER guidelines, with WISER consultants available for additional help if needed. The sensors cover only the network layer and basic sensor management functionality.

Dashboard: reports high-level charts and diagrams which provide valuable at-a-glance information about sensor variables and incidents detected by the monitoring infrastructure. Professionals without IT security expertise can use it to make informed decisions based on the information available.

Online service support: WISER team of consultants with considerable expertise on cyber security and specific knowledge about the WISER Framework.

WISER promotional message for CWE

Who: Businesses and public organisations who follow a company-wide/board-level approach to cyber risk management; SMEs that are high risk/rewards for cyber criminals, including SMEs connected to the IT systems of larger companies.

Why: The growing number of connected devices and people is bringing many business benefits and opportunities, but also an increasing number of cyber-attacks with direct financial losses and indirect effects, such as reputational damage. Companies of all sizes should approach cyber risk as a business risk
Today's fast-evolving threat landscape calls for a company-wide approach to cyber risk management. It also calls for cyber security service packages that can react quickly and enable companies to make an informed decision about mitigation actions.
What: CyberWISER Essential helps organisations counter the threat of cybercriminals. Companies can detect, monitor and asses their IT vulnerabilities in real time. This helps them turn threat intelligence into key business decision-making actions. Real-time assessment helps detect vulnerabilities in the IT system with valuable insights about indirect impacts of a cyber-attack. The Dashboard enables continuous monitoring through graphs and trends. The Decision Support System provides basic mitigation measures based on recognised best practices and WISER expertise.

6.1.3 CyberWISER Plus – Online package and onsite services for company-wide cyber risk management

In this section, we draw on the positioning of WISER in D2.6, Section 2.

The self-assessment questionnaire collects inputs on the business profile, the ICT profile, and infrastructure elements to allow the services to create a more complex and elaborate correlation between IT- and business-related risks.

Vulnerability testing: broader range of vulnerability scanners enables the detection of a wider range of vulnerabilities compared with CWL.

DSS societal impact evaluation: ranks and prioritises the mitigation measures based on societal or indirect impacts (defined in D8.3 as tangible and intangible). As the societal impact is closely related to reputational damage (intangible), which, can have a very negative effect on the company's finances (see Case Studies on TalkTalk and Yahoo!). This WISER feature contributes to raising awareness about one of the aspects of the cyber risk that is usually neglected, and which is stressed in CW-SEIT.

Real-time monitoring: A Security Information and Event Management (SIEM) solution and a correlation engine that continuously analyses security events, aggregating data from many sources. Combined and correlated data generates reports and alerts.

Real-time risk assessment: high degree of customisation and wide range of inputs as the information available has both high quantity and quality and the models used are more complex. In addition, it features a cost-benefit analysis of the mitigation measures generated by the Risk Assessment Engine.

Risk Modelling system: a widget of a risk model library, enabling the user to download, change and upload a new risk model relevant to the company.

Sensor installation: WISER sensors and agents are installed in the IT infrastructure to detect potentially harmful events and vulnerabilities. The customer installs the sensors and agents using the WISER guidelines, with WISER consultants available for additional help if needed. Sensors cover both the network layer and the application layer. In CyberWISER Plus the scope of the sensors covers not only the network layer, but also the application layer. The monitoring and testing techniques produce high-quantity and high-quality data collected from the target infrastructure. It also enables location of customised sensors tailored to the specific nature of the target infrastructure and integrates existing sensors provided to the customer, which requires the involvement of the WISER team.

Dashboard: reports high-level charts and diagrams which provide valuable at-a-glance information about sensor variables and incidents detected by the monitoring infrastructure. Professionals without IT security expertise can use it to make informed decisions based on the information available.

Cost-benefit analysis: The main advantage of cost-benefit analysis is that companies can rank and prioritise measures based on the rates provided. CyberWISER Plus represents a novelty for senior management which usually lacks this information, preventing informed decisions that are gaining in importance. In practice, it means that managers no longer need to put their trust in other criteria or implement measures with reduced scope but that require big investments. CyberWISER Plus helps you steer the company security policy.

Online service support: WISER team of consultants with considerable expertise on cyber security and specific knowledge about the WISER Framework, combinable with onsite support.

Onsite service support: Providing an extra layer of advanced support for specialised set up and tailored configuration.

WISER promotional message for CWP

Who: Businesses and public organisations who follow a company-wide/board-level approach to cyber risk management; SMEs that are high risk/rewards for cyber criminals, including SMEs connected to the IT systems of larger companies. It targets those organisations that need to make a cost-benefit analysis and require technical expertise in installing package features.

Why: Cyber risks are business risks that have both direct economic impacts but also indirect effects on a company's reputation, eroding customer trust. Traditional risk assessment processes can take days to provide results and are not fit for today's fast-evolving cyber threat landscape.

What: CyberWISER Plus enables companies to detect, monitor and manage in real time vulnerabilities in their IT systems.

Service package features

- Real Time Monitoring and Real Time Risk Assessment: a cost-benefit analysis and an assessment of indirect impacts based on your risk profile.
- Dashboard: crucial at-a-glance information about cyber risks, vulnerabilities and incidents detected, helping you track real risks.
- Decision Support System Cost benefit analysis: comparing and ranking different mitigation measures that can be taken against cyber threats.

- Cost-benefit analysis helping companies rank and prioritise measures as a novel approach that does not require big investments.
- WISER Online and Onsite Service Support from a team of cyber security experts.

6.2 CW-SEIT and the 6-month WISER Sprint

The figure below shows the timeline for the rollout of CW-SEIT and how WISER will intensify its marketing activities in the next 6 months with particular reference to CW-SEIT.

Figure 6: Timeline for CW-SEIT

July-early September 2017

- While SW development gets underway, WISER will create a dedicated page for SMEs on the importance of cyber risk management with selected insights and teasers for the tool extracted from this report.
- Interactions with representatives from business associations and cyber security clusters (multipliers) will already highlight the forthcoming tool, with specific reference to business benefits to garner support and gauge member interest (supported by T6.5).
- Upon rollout in July 2017, WISER will embark upon a major promotional campaign, spanning its SME network, SMART social media campaigns, a press release, requests for support from business associations and cyber security clusters.
- The rollout of the final cartography in July (D6.10) is also an opportunity to package this tool, the translated glossaries and guides, and CW-SEIT in special campaigns around getting ready for GDPR linking both the importance of risk management and the requirement to report to competent authorities, the details of which are provided in the cartography. This activity will continue through to November 2017.

Mid-September-November 2017

- The intensive marketing campaigns will continue, aiming to identify champions of the tool through WISER multipliers. This includes messages in partner languages.
- The strategic plan for WP8, as reported in D8.6, includes WISER active participation at carefully selected events to showcase CW-SEIT and the service packages, leveraging F2F interactions also with SMEs and other CW-SEIT targets for hands-on sessions and the collection of testimonials.
- Continued liaison with multipliers to encourage back-links and announcements to members encouraging them to use the tool.

- The final event in October will offer another opportunity to promote CW-SEIT.
- Mid-October impact assessment checkpoint on its impact, including any potential new leads identified and resulting increases in use of CWL. Adjustments can be made, if necessary, to the promotional plans.

November 2017

- WISER exploitation plans defining how CW-SEIT will be sustained, including potential for future developments.

7 Conclusions and Next Steps

D8.3 presents a new approach to CW-SEIT based on an extensive review of V1.0, an updated analysis of the cyber risk landscape and direct interaction with SMEs, which have little understanding of the risks they are facing, let alone the resources to implement a risk management strategy.

CW-SEIT V2.0 fills this important gap by offering a tool that is more pragmatic and business-friendly compared with V1.0. While this requires new software development for delivery of the tool in July 2017, the new version also strengthens the WISER go-to-market strategy by guiding the user on cyber risk management and the CyberWISER service packages, as defined in D2.3. CW-SEIT also supports the portability to other verticals in WP7 through the collection of data on potential customers in Q1-4 of the questionnaire.

At the same time, we include references to our glossaries and guides available in different partner languages and also features of the WISER cartography to help businesses comply with the GDPR in terms of notification to competent authorities.

In fact, an important feature of the CW-SEIT V2.0 is helping EU businesses prepare for the new regulation, where risk management assumes even greater relevance.

Another value-add of D8.3 comes from the wealth of independent insights gathered from the analysis, including the case studies that illustrate the wide range of potential socio-economic impacts. These insights are presented in business-friendly terms and can now be used as core messages for WISER communication tools, from the website and social media, to promotional material and press kits, as defined in D8.6.

Next steps include:

- SW enhancements start mid-June for rollout in late July 2017. During this time, WISER will create a dedicated page for SMEs on the importance of cyber risk management with selected insights and teasers for the tool extracted from this report.
- Upon rollout, WISER will embark upon a major promotional campaign, spanning its SME network, SMART social media campaigns, a press release, requests for support from business associations and cyber security clusters.
    - This activity will continue through to November 2017.
- The rollout of the final cartography in July (D6.10) as an opportunity to package this tool, the translated glossaries and guides, and CW-SEIT in special campaigns around getting ready for GDPR linking both the importance of risk management and the requirement to report to competent authorities, the details of which are provided in the cartography.
- Interactions with representatives from business associations and cyber security clusters (multipliers) will already highlight the forthcoming tool, with specific reference to business benefits to garner support and gauge member interest (supported by T6.5).
- The strategic plan for WP8, as reported in D8.6, includes WISER active participation at carefully selected events to showcase CW-SEIT and the service packages, leveraging F2F interactions also with SMEs and other CW-SEIT targets for hands-on sessions and the collection of testimonials.
- WISER exploitation plans defining how CW-SEIT will be sustained, including potential for future developments.