The HERMENEUT Project: Enterprises Intangible Risk Management via Economic Models based on Simulation of Modern Cyber Attacks

Enrico Frumento[1] and Carlo Dambra[2]
[1]*CEFRIEL Scarl, Politecnico di Milano, Viale Sarca 226, Milano, Italy*
[2]*ZenaByte S. R. L., Via Opera Pia 11A, Genova, Italy*

Keywords: Targeted Attacks, Intangible Assets, Cyber-risk Estimation.

Abstract: This paper presents the funding principles of the HERMENEUT H2020 EU project (www.hermeneut.eu), whose objective is to assess cyber-risk and valuing consequences on both tangible and intangible assets. HERMENEUT innovates with a unique cyber-security cost-benefit analysis approach that combines current attack trends, integrated assessment of vulnerabilities and likelihoods of cyber-attacks with an innovative macro- and microeconomic model of intangible costs, to deliver risk estimations for individual organisations, sectors and the economy. It then suggests options to both apportion cyber-security budget on multiple mitigations and transfer non-tolerable residual risks to cyber-insurance. HERMENEUT also provides a decision support tool to stakeholders and validates it in two industries belonging to two sectors increasingly under cyber-attack: health-care and an Intellectual Property-intensive sector. The HERMENEUT project is now in its second year of life, heading to the proof of the theoretical funding assumptions in the field-tests.

1 INTRODUCTION

Today, the elusiveness of targeted attacks (TAs) (Trend Micro, 2015) and the number of evasion tactics exploited by the ongoing attacks are so large that monolithic defence strategies are not still efficient. Successful attacks are built to stay under the detection threshold on all the layers of the security (from network to the human layer): e.g., network scanning is usually today a feeble activity, systems' compromising happens with ad-hoc copies of unique malware, and phishing campaigns are tailored around single humans (DOGANA, 2018) (ProofPoint, 2018). Cybercrime is increasingly going in the direction of sophisticated "low-and-slow" attacks (Johnson, 2016). The low-and-slow approach involves attackers remaining invisible for as long as possible, while stealthily moving from one compromised host to the next without generating regular or predictable network traffic patterns or data exfiltration purposes as they hunt for specific data or system targets. The rapidity of the single attack steps is one crucial element of being stealthy.

The defence paradigms therefore must adapt to this increasingly flexible and feeble scenario, where the usual defence systems based on pattern recognition are not effective anymore. As an example, ad-hoc malware exploits this model adopting 1:1 infection scheme to remain unnoticed for a long time. As a result, a recent report from FireEye cites "*the average time from an email phishing breach to detection is 146 days globally, and a colossal 469 days for the EMEA region*" (FireEye, 2017). The early detection of the weak signals of an ongoing attack is one important challenge in today's security market. One promising approach to this challenge is the adoption of Artificial Intelligence (AI) to analyse the data with the objective to capture emerging and unnoticed patterns/trends. In addition, Cyber Threat Intelligence (CTI) tools are facing this challenge. However, in this second case, the most problematic issues is not the complexity of the evaluation models but the potentially uncontrollable divergence of their forecasts. CTIs preciseness is tied to the preciseness of the Indicator of Compromise (IoC), whose collection is regulated through different bodies (mainly EU such as the ISACs (ENISA, 2018) or crowd-based efforts such as VERIS CDB (VERIS, 2018)) and supporting (usually de-facto) technologies (STIX being the reference serialization language

Frumento, E. and Dambra, C.
The HERMENEUT Project: Enterprises Intangible Risk Management via Economic Models based on Simulation of Modern Cyber Attacks.
DOI: 10.5220/0007413504950502
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 495-502
ISBN: 978-989-758-359-9

(STIX, 2018)). What limits CTIs is, therefore, the instability of their forecast models, which require efforts to collect IoCs, elaborate and distribute the early alerts. These limitations go beyond the possibilities of an organisation with low-budget security programs.

For the above reasons, the EU set up a significant effort in keeping secure and coherent information sharing and feeding the forecast models with correct data. The achievement of this objective happens through legal reporting obligations (see the GDPR) and organisations at national or EU levels (Computer Emergency Response Team, CERT, Computer Security Incident Response Team, CSIRT and sectorial Information Sharing and Analysis Center, ISAC). However, this mechanism is not still wholly deployed; the costs and technical/organisational efforts to fully integrate into the EU cybercrime forecast infrastructure, for a company with a low-budget security program, are still relatively high (also concerning required competencies). HERMENEUT aims to bridge the gap for organisations with low-budget security programs, creating an "agile" service, yet with some approximations, immediately exploitable to get insights and criteria for the cyber risk mitigation. On the other hand, the described infrastructure and IoCs are covering almost only tangible/technical indicators of an ongoing cyber-attack. The world of intangibles is still mainly not covered (e.g. only data leaked are) by the EU information collection infrastructure and forecast models.

2 CONTEXT

As reported by (Ahmed, 2017) the current approaches to IT security and risk management tend to underestimate the following key aspects:

- The human factor (covering subjective, organisational, societal and economic aspects) in the identification of vulnerabilities to cyber-attacks. This aspect is often ignored even though, as recently demonstrated (DOGANA, 2018), Social Engineering 2.0 (SE) attacks generate the highest costs in terms of both consequences of and protection against attacks (ProofPoint, 2018) (ENISA, 2017). The ease of creating fraudulent social media accounts for known brands drives a clear preference for phishing in social media-based attacks, though other types of media are also abused for the same purpose. Distinguishing fraudulent social media accounts from legitimate ones is often tricky, and they are numerous: a recent white paper (ProofPoint, 2018) reports that 40% of Facebook accounts and 20% of Twitter accounts claiming to represent a Fortune 100 brand are unauthorised.
- The strategy of the attacker in the identification of vulnerabilities and assets at risk. Modern attacks follow the same business logic as that followed by big companies that involve multidisciplinary competencies in the definition process of their strategies and business plans (Thomas, et al., 2015) (ENISA, 2017) (ProofPoint, 2018). The same multidisciplinary approach combining engineering, risk assessment, economic, cognitive, behavioural, societal and legal knowledge is needed to address the strategy of professional IT attackers properly.
- The role of intangible assets in the quantification of the consequences of cyber-attacks. As reported in (Kerber & Jessop, 2015) "*More than half the value of companies worldwide is in intangible assets, such as intellectual property, much of which is stored on computers and could therefore be vulnerable to hackers. That figure could be as high as $37.5 trillion of the $71 trillion in enterprise value of 58,000 companies, according to Brand Finance,*

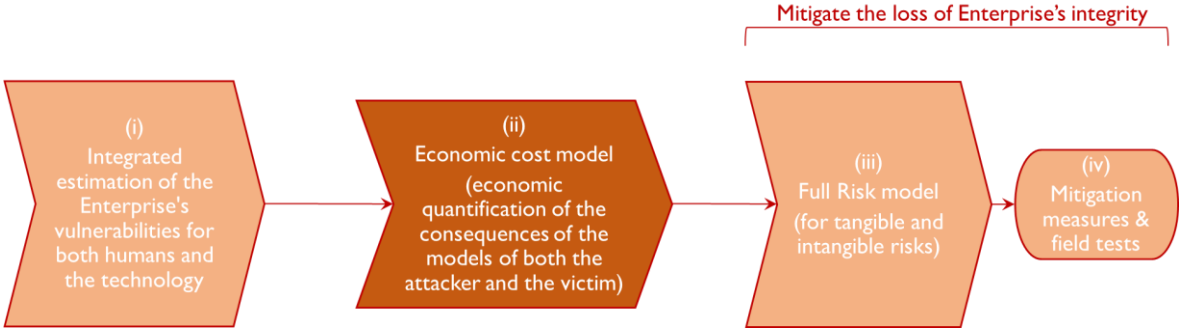

Figure 1: Logical high-level view of the HERMENEUT approach.

a consultancy specialising in the valuation of intangible assets". Moreover, according to (PAYCHEX, 2016), more than 70% of attacks target small businesses, and as much as 60% of hacked small and medium-sized businesses go out of business after six months.

Several sources report that estimates of the cost of cyber-crime are not accurate enough. For example, ENISA: "*the measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task*". Analysing the past cyber-attacks (Deloitte, 2016) (Ponemon, 2018) (Zurich Insurance, 2014), it is possible to observe that a successful cyber-attack may lead to several consequences for the victim organisation:

- **Direct Consequences:** the (partial or entire) loss and/or compromise and/or damage of one or more tangible and/or intangible assets as the direct effect of the cyber-attack.
- **Indirect Consequences:** the direct consequences of the attack may generate, as a cascade effect, other losses in the tangible and/or intangible assets of the organisation (e.g. theft of personal data from a credit card company may generate a loss of reputation and as a further consequence a loss of clients).
- **Attack-related Costs**: beside the direct and indirect consequences, being the victim of a cyber-attack generates other costs, including those reported in Table 1.
  The impact tree with tangible and intangible assets together and the possible attack-related costs is shown in Figure 2.

Table 1: Attack-related costs.

Before-the-attack status restoration (service, data, etc.)	Cyber-security restoration/improvement
Legal/litigation costs and attorney fees	Notification and regulatory compliance costs
Liability costs	Customer breach notification costs
Post-breach customer protection/care costs	Lost customers recovery
Public relations	Increase of insurance premiums
Loss of revenues	Increased cost to raise the debt
Value of lost/not fulfilled contract revenues	

2.1 The Role of Intangibles in Nowadays Attacks

As mentioned in the previous sections, the role of intangible assets is an often-neglected element for the quantification of the consequences of cyber-attacks. The consequences of data breaches in terms of impact on tangible and intangible assets are a problem studied since several years (Riddle, et al., 2011). Cyber-attacks can damage physical – tangible – assets of the victimized institutions, e.g. turbines destroyed because of the manipulation of its control systems (Langner, 2013). More frequently, though, the damage will not be physical. Increasingly the attacks are hitting intangible assets as a primary target (e.g. automated cyber *crowdturfing* attacks (Yao, et al., 2017)) or, because of an attack, (e.g. Uber data breach in 2017). For example, "Crowdturfing," is a combination of "crowdsourcing," meaning recruiting large numbers of people to contribute a small effort each toward a big task (like labelling photos), and "astroturfing," meaning false grassroots support (in the form of bogus reviews or comments, for example) (Jacobs, 2014).

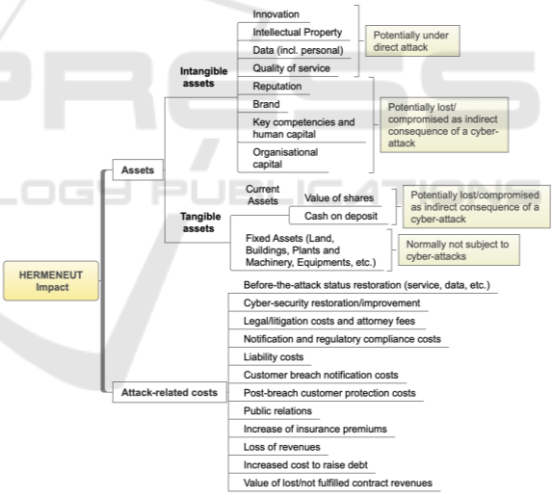

Figure 2: HERMENEUT impact tree.

Modelling these attacks is difficult for the relative "obscurity" of the cybercriminal attack plan.

Intangible Assets (i.e. reputation, trust in the organisation, patents, trademarks, knowledge, expertise, human capital, etc.) are now recognised as critical to the performance of companies and nations. At the macroeconomic level, many studies stress the dominant nature of intangible investment as well as its essential contribution to economic growth and productivity (Nakamura, 2003). At the microeconomic

level, besides research, which focuses on specific intangibles such as R&D, patents or brands, studies also stress the importance of intangibles assets for corporate performance, using a comprehensive approach (Ahmed, 2003). Intangibles often contribute to 80% of the value of organisations.

3 THE HERMENEUT APPROACH

Given the described scenario, HERMENEUT aims to create an inclusive approach to cyber-security cost-benefit analysis. The approach: (i) starts from an integrated assessment of vulnerabilities and their likelihoods, (ii) exploits an innovative macro- and microeconomic model for intangible costs and ends (iii) with an estimation of the cyber-risks for an organisation or business sector followed by guidelines (iv) on investments, to mitigate the loss of an enterprise's integrity.

The HERMENEUT core model reported in Figure 1represents the following fundamental steps:

1. Integrated estimation of the enterprise's vulnerability, for both humans and technology
2. Development of an economic cost model that quantifies the consequences of attacks for both, attackers and victims
3. Development of a full risk model for both tangible and, especially, intangible risks
4. Mitigation measures for the loss of enterprise's integrity, with particular emphasis on two business sectors (Healthcare and IP-intensive Industries, as defined by the (European Patent Office, 2013))Development of a decision and policy-making tool supporting cost-benefit risk-based investments in cyber-security mitigation (including cyber-insurance). The tool, leveraging on an Open Source risk assessment framework, integrates the models and the knowledge created in the project. It provides the users (i.e. decision-makers in cyber-security cost-benefit analysis and protection measures) with novel functionalities for (i) the estimation of tangible and intangible costs generated by cyber threats and (ii) risk-based and cost-based analysis and assessment of proper countermeasures for protection

As defined in many standards (e.g. (International Organization for Standardization, 2009)), risk can be defined as the combination of the likelihood of an event to occur and its consequences. When assessing the risk of cyber-attacks for an organisation, difficulties are concentrated into the following aspects:

- Estimating the vulnerabilities of the organisation to cyber-attacks and therefore the likelihood of being subject to these attacks and the tangible and intangible assets at risk, as a direct or indirect consequence of the attack. Since it is impossible to estimate the likelihood of a cyber-attack to a specific organisation directly, it is necessary to assess the technical and social vulnerability of the organisation and indirectly compute the probability of the cyber-attack.
- Quantifying the possible consequences of the attacks on the tangible and intangible assets at risk. It is of particular importance to take into consideration the role that intangible assets can play, since their costs, often neglected can be as large as tangible one or exceed these.
- Assessing the risks and taking decisions on the best-possible investments to mitigate the risks of cyber-attacks.

Moving from the organisation level to the industrial sector level, it is crucial to define policies and recommendations for stakeholders to adapt to and

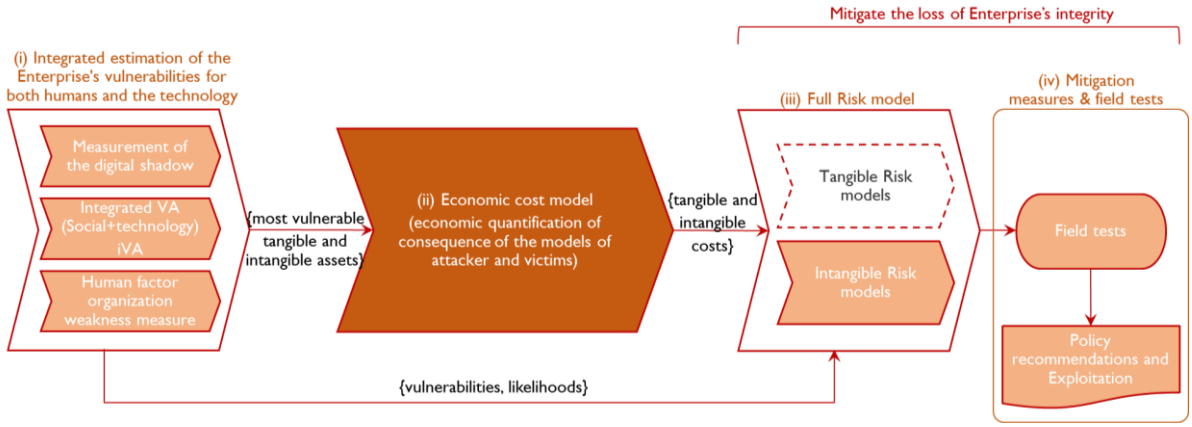

Figure 3: The HERMENEUT concept.

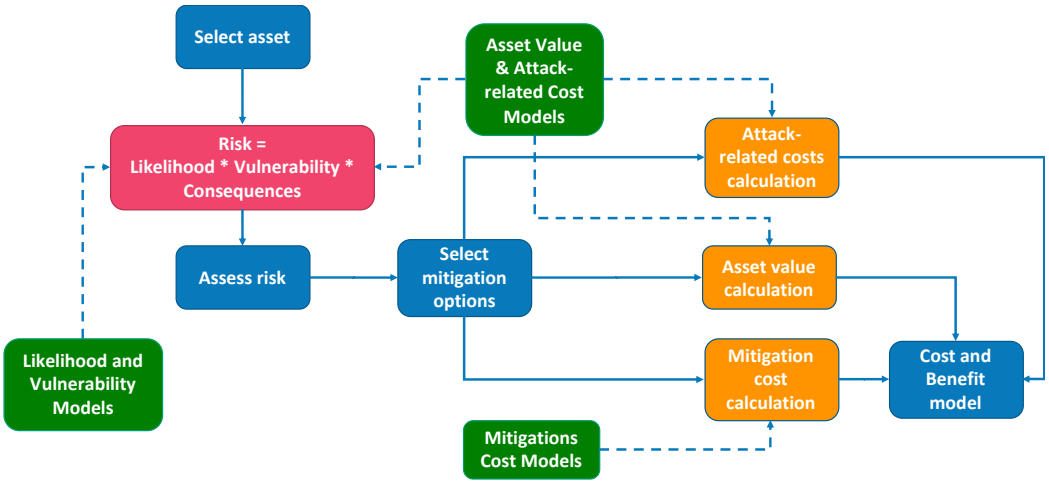

Figure 4: The HERMENEUT risk assessment approach.

protect from the continuously changing cyber-risks; having a clear idea – for each sector – of the most common vulnerabilities and the potential consequences on the assets at risk.

Therefore, HERMENEUT is proposing an inclusive approach to cyber-security, addressing the problem, not only from the technical point of view, but also introducing societal, institutional and economic perspectives, as illustrated in the diagram in Figure 3 represents the general HERMENEUT model and adds, to what already shown by Figure 1 a detailed view of the phases from (i) to (iv).

The role of the phase (i) is to detect the vulnerabilities and their likelihood, simulating the modern threat landscape through an integrated estimation of the enterprise's vulnerabilities, for both humans (through social engineering simulations and social driven vulnerability assessment) and technology (e.g., simulating the modern ad-hoc threats). This phase feeds the phase (ii), the HERMENEUT's economic cost model and the phase (iii) the HERMENEUT's full risk model. The phase (iv) conjoins the results of the prior phases by deriving specific mitigation measures & field tests for the selected business sectors.

The inclusive HERMENEUT approach is based on:

- An Integrated estimation of the enterprise's vulnerabilities for both the humans and the technology (phase (i)) and the corresponding tangible and intangible assets at risk, considering the business plan of the attacker, the commoditisation level of the target organisation, the exposure of the target and finally the involved human factors and, on the same basis, to estimate the likelihood of a potential cyber-attack exploiting the assessed vulnerabilities. The resulting methodology is called integrated Vulnerability Assessment (iVA). This improved assessment considers the business plans of the attacker, the commoditisation level of the target organisations and its exposure, the relevant cognitive, psychological and social factors.
- An innovative micro- and macroeconomic cost model focusing on intangible costs (phase (ii)) able to quantify the cost of the loss of one or more – especially intangible – assets at risk identified by the phase (i) based on an eclectic view of the role of intangibles by considering the impact of intangible factors and cyber-risk on organisation's sustainability at the micro-economic level and by considering the size of the GDP sensitive to cyber-risk at the macroeconomic level.
- A inclusive risk assessment model (phase (iii))– taking as input the vulnerabilities and likelihoods of cyber-attacks from the iVA and the economic quantification of potential consequences from the cost model – able to support decisions related to information security investments on hard (traditional) and soft mitigation measures (awareness and training, cyber-insurance, reorganisation of security procedures, etc.).
- Verification in two specific business sectors (Healthcare and IP-intensive industry) of the developed models (phase (iv)).

To complete the actions HERMENEUT uses a KISS (Keep It Simple and Stupid) approach presenting less information possibly but making the whole process more accessible to compile and less prone to inaccurate answers. This is supposed to avoid the problems of past methods based on long and complex questionnaires or profiling, the quality of whose answers usually degrades along the compilation

3.1 The Assumptions of the Model

HERMENEUT research statement has several commonalities with the CTI world but also some approximations that differentiate it. HERMENEUT defines itself as a Strategic CTI, according to the classification reported in Figure 5. As such, the main functionality offered by HERMENEUT is to inform the CISO or the management board of an organisation with high-level information on changing risks.

Figure 5: Cyber Threat Intelligence Subtypes (source (Chismon and Ruks, 2015)).

However, HERMENEUT is not a mitigation measure, but rather a decision support tool, which includes an integrated cyber risk and economic model for the tangible and intangible asset losses. Although some of its elements come from the CTI world, the level and complexity of the model are very different. HERMENEUT aims to give a reasonable risk evaluation model for organisations with low-budget security programs because of the approximations introduced. The project intends to:

1. ease the adoption, of a safer cyber posture and more predictive reactions, without diminishing the quality of the forecast models,
2. ease the long-term inclusion of organisations to the EU CTI-based prevention model while managing the tangible and intangible assets in a unique conceptual framework

These assumptions lead to several optimisations:

- The collection of evidence and the positioning goes through questionnaires typically compiled by the CISO. This collection process poses limits and biases the quality of data collected. The research hypothesis is that these approximations are not affecting the advantages of an immediately available solution for the estimation of the cyber risk.
- The inference engine is not using AI but rather a deterministic algorithm (probability-based risk evaluation).
- HERMENEUT overcomes the limited update frequency of CAPEC (once a year) by proposing custom dynamic solutions for the proactive risk re-assessments and refinement models based on past experiences and dark web data.
- The attack strategies described with STIX and defined by CAPEC have been simplified and grouped to be manageable by an average CISO, but also to not surpass the quality of the information collection tool used (i.e. questionnaires).

A confirmation of the expected usefulness of the HERMENEUT system comes from the recent data of a survey from SolidWorks (SolidWorks, 2018): "*more than one-third of US organizations (37%) face security risks that exceed their overall security maturity. Within that group, 10% face a deficiency when it comes to protecting themselves from the threats in their environment*". A portion of the funnelling process of the HERMENEUT framework is about the assessment of the organisation maturity. Of the several maturity models currently in existence, the one used by HERMENEUT is simplified to rapidly offer an evaluation that organisations can take to benchmark their maturity. Cybersecurity leaders who complete the HERMENEUT online tool receive a report that scores the organisation's risk and helps to shape the future behaviours. However, the research questions of HERMENEUT are not preventing the future collaboration of HERMENEUT with the CTI community. The central hypothesis that the project wants to prove is the correctness of the assumptions made and their context of validity. The estimates reported above matches the preciseness of the economic and risk models, especially for the intangible assets.

3.2 3-Levels HERMENEUT Risk Assessment Methodology

The proposed methodology, and its refinement to include intangible assets is based on a standard risk assessment approach compliant with the following standards

- ISO 31000 "Risk management" (Organisation, International Standardisation, 2009)
- ISO 31010 "Risk management – Risk assessment techniques" (International Standardisation Organisation, 2009)

Nevertheless, the aspects arising from the tangible and intangible assets are the focus:

- How to integrate the cost-benefit analysis into the overall risk assessment methodology,
- The inclusion into the approach of the various intangible assets' aspects (e.g. loss of reputation, risk perception, awareness as mitigation, etc.).

HERMENEUT risk assessment is a three phases-levels funnel, where each level goal is to increase the

confidence of the measure, besides it also adds estimation of the connected costs. The project outlined the criteria and boundaries, as reported in Figure 4:

- Level 1: Conservative (Screening) Risk Assessment. System vulnerability assessments are carried out using the results of data collection and findings from the iVA, followed by risk evaluations using ranking techniques and then setting priority on remedial and preventive measures. This step is fundamental to start the prioritisation of resources.
- Level 2: Qualitative (secondary) Risk Assessment. The assets are requiring further consideration and having positive cost-benefit implications need additional data. These data allow for the reduction of uncertainty and more robust risk assessment. Boston-square methods and specific vulnerability metrics are used alongside data elicitation from experts.
- Level 3: Quantitative (Mainly Probabilistic) Risk assessment. This aspect is usually needed for the most critical and complex assets. The level of detail depends on the uncertainty and models' requirements. This one is the most significant level regarding costs for the company, to collect the required information.

4 EARLY EXPERIMENTS

HERMENEUT concentrates on two selected areas: IPR and healthcare. Healthcare trials started earlier with two providers, who are involved in the entire validation process. Being the healthcare sector very complex and involving several actors, we performed a selection to identify providers with different characteristics for broad coverage. The first one is a private clinic, operating in Italy with some detached departments/services. The second one is a public healthcare provider, operating in two different cities in Tuscany with strong research activities and an IT department, which develops software for other regional public healthcare institutions.

In both cases, the project consortium performed questionnaires, focus groups and interviews with the company's CISO, following the developed methodology, to identify the most significant assets, the threats and the cascading effects of a cyber-attack. In both cases, the focus was on the patients' health data and the consequences of its theft or counterfeit. In the private case, more importance was given to the cash, due to its importance for the daily operational capacity of the structure, while in the public case more importance was given to the IPR, following the good reputation of the structure in SW development and research. The results are summarised in a series of loss diagrams, such as in Figure 6 (the complete results will be in the project's deliverables, available on its web site). These initial *loss diagrams* are preliminary and still needs a formal assessment with the company's internal management.

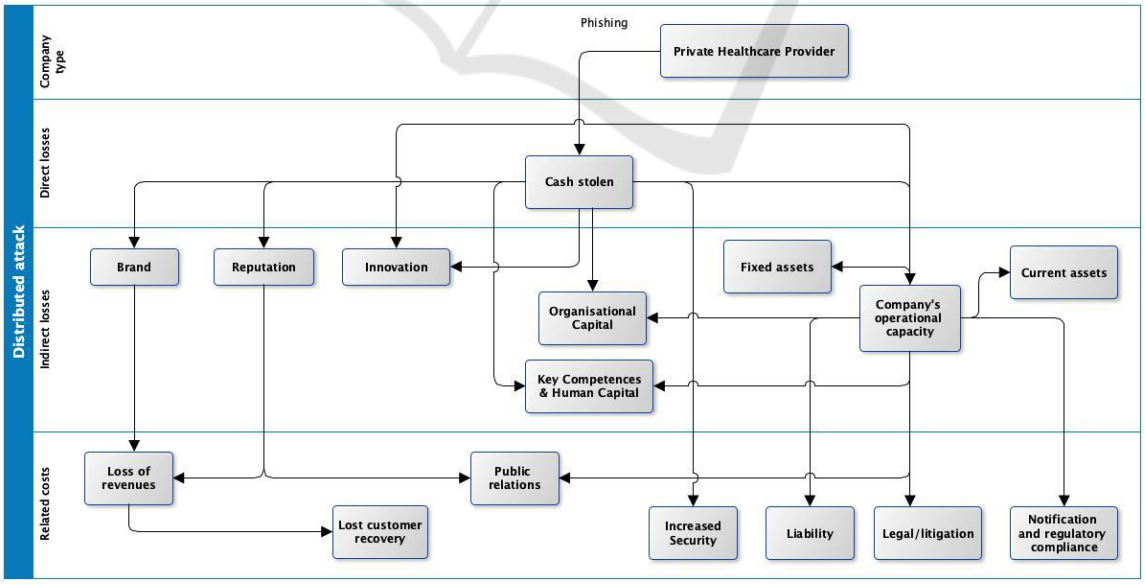

Figure 6: Losses generated to a Private Healthcare Provider by a Phishing attack with cash stolen.

5 FUTURE DEVELOPMENT

HERMENEUT is a *knowledge-extraction funnelling process*, which measures the cybersecurity posture of an organisation from the knowledge of its internals (employees and C-levels) using questionnaires, to support their cyber-risk management. Questionnaires supported processes (e.g. also most Capability Maturity Models), has biases leading to approximations that we want to verify. As shown in Figure 7 data quality/accuracy is directly proportional to time and cost. The different measurement methods are valid within limits above which the knowledge acquired or, the required preciseness degrades. HERMENEUT still has to understand its limits. A more robust solution would use a mixed approach, questionnaires plus technical evidences collection (e.g., using penetration tests). However, the advantage of questionnaire-based or mixed approaches is the saving of costs.

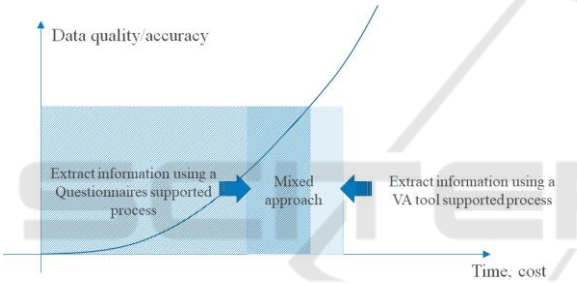

Figure 7: Data quality/accuracy vs time,costs and knowledge extraction method used.

HERMENEUT will open source in 2019 its framework, tested in the Healthcare and IP-intensive industries. The choice is a consequence of the imbalance between the effectiveness of recent attacks, the increasing number of those hitting the intangibles and the relative inadequacy of the defences.

ACKNOWLEDGEMENTS

Funded under the EU H2020 HERMENEUT project, grant agreement No. 740322.

REFERENCES

Ahmed, B., 2003. *The management of intangibles: The Organisation's most valuable assets.* London: Routledge.

Ahmed, B., 2017. *Micro - and macroeconomic modelling of intangible cyber-costs.*

Chismon, D. and Ruks, M., 2015. Threat Intelligence: Collecting, Analysing, Evaluating.

Deloitte, 2016. *Beneath the surface of a cyberattack A deeper look at business impacts.*, s.l.: s.n.

Dogana, 2018. *DOGANA Project.* [Online] Available at: www.dogana-project.eu

Enisa, 2017. *Threat Landscape Report.* [Online].

Enisa, 2018. *Information Sharing and Analysis Centres (ISACs): Cooperative models.* [Online].

FireEye, 2017. *Cyber Threats: A perfect storm about to hit Europe?.*

International Organization for Standardization, 2009. *ISO 31000 Risk management — Principles and guidelines.* s.l.:s.n.

Jacobs, J., 2014. *Fake Followers for Hire, and How to Spot Them.*

Johnson, M., 2016. *Cyber crime, security and digital intelligence.* London: Routledge.

Kerber, R. and Jessop, S., 2015. *Asset Managers Urged to Make Cyber Risk Top Priority.* [Online].

Langner, R., 2013. *To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve the Langner group.* London: Routledge.

Nakamura, L., 2003. A Trillion Dollars a Year in Intangible Investment and the New Economy. In: *Intangible Assets.* Oxford: Oxford University Press.

Paychex, 2016. *Creating a Cyber Security Culture in Your Business.*.

Ponemon, 2018. *Cost of Data Breach Study.*

ProofPoint, 2018. *Protecting People Report. A quarterly analysis of highly targeted attacks.*

ProofPoint, 2018. *The Human Factor - People-centred threats define the landscape.*

Riddle, B., Nyman, N. and Rees, J., 2011. *Estimating the costs of a data breach: An exercise at the new Hampshire state cancer registry.* Atlanta, s.n.

SolidWorks, 2018. *Secureworks Launches First Cybersecurity Maturity Model Based on an Organization's Inherent Risk.*

Stix, 2018. *A structured language for cyber threat Intelligence*

Thomas, K. et al., 2015. *Framing Dependencies Introduced by Underground Commoditization.* s.l., s.n.

Trend Micro, 2015. *Understanding targeted attacks. What is a targeted attack.*

Veris, 2018. *Community Database.*

Yao, Y. et al., 2017. Automated Crowdturfing Attacks and Defenses in Online Review Systems. *Arxiv.org.*

Zurich Insurance, 2014. *The good, the bad and the careless. An overview of corporate cyber risk.*, s.l.: s.n.