Capability oriented RE for Cybersecurity and Personal Data Protection: Meeting the challenges of SMEs

Evangelia Kavakli
Institute of Digital Innovation & Research (IDIR)
Dublin, Ireland
evangelia@idir.eu

Pericles Loucopoulos
Institute of Digital Innovation & Research (IDIR)
Dublin, Ireland
peri@idir.eu

Yannis Skourtis
Institute of Digital Innovation & Research (IDIR)
Dublin, Ireland
yannis@idir.eu

Abstract— **SMEs face multiple challenges related to cybersecurity and personal data protection. Prominent amongst these challenges is the lack of appropriate guidelines addressing specific SME requirements. The proposed RE methodology aspires to bridge this gap by establishing a generic process specifically targeting SMEs needs and capabilities. This paper describes the conceptual foundation of the methodology and reports on the way that the theoretical foundations were applied on an SME offering social care services.**

Keywords—capability, requirements, security, privacy, SMEs

I. Introduction

Security contributes toward ensuring that processing, storing, and communicating information sufficiently protects *confidentiality*, *integrity*, and *authenticity* (a triad often referred to as CIA). Enterprises, regardless of their size, must manage the Cyber Security (CS) risks to improve the security and resilience of their assets as well as ensuring Personal Data Protection (PDP). In the case of Small to Medium size Enterprises/ Micro Enterprises (referred to henceforth collectively as SMEs) additional challenges present themselves because of lack of resources and of relevant in-house expertise [1]. The work presented in this paper seeks to address the requirements-specific challenges for these situations, focusing on (a) the foundational parts of a capability-oriented Requirements Engineering (RE) methodology intended to assist SMEs and on (b) demonstrating the way that this methodology is practically applicable using a real-life use case. The methodology, known as "SCORE" builds upon earlier work, known as e-CORE (early Capability Oriented Requirements Engineering) [2] and is being used in the SENTINEL project[*]. It proposes a systematic process whose focus is to answer the question of "*what kind of capabilities are required for SMEs to obtain enterprise-grade security and personal data protection?*".

Space restrictions limit the amount of details regarding the methodology and its application that can be included in this paper. Nevertheless, the backbone of the methodology is presented in terms of its conceptual foundation, the graphical presentational elements that are used to help the stakeholder visualize the captured elements and the way of working, using examples from a use case involving an SME that handles critical personal data. The paper is organized as follows. Section II provides a brief overview of the aforementioned challenges. Section III discusses the background to capability oriented RE whereas section IV introduces the conceptual foundations of the SCORE approach. To demonstrate the way that SCORE is used, an overview of its application on a pilot case is provided in section V. Section VI reports on on-going research into assisting SMEs for profiling their CS and PDP capabilities and carrying out self-assessment. Finally, section VII concludes this paper with a short reflection on achievements to date and on future work.

II. Addressing the CS and PDP Challenges to SMEs

SMEs with limited personnel and resources face difficulties in dealing with the risks associated with the development of their technologies and their impact [3]. Despite the constant adaptation of new technologies, the level of SMEs information security and privacy standard adoption is relatively low. One of the biggest risks SMEs face is exposure of users' personal data (data breach), which could lead to the loss of the reliability and trust between the company and its customers and, more importantly, adversely affect the freedoms and rights of the individuals whose data is exposed [4]. In a recent ENISA study, investigating 249 SMEs EU-wide for their overall CS awareness and related concerns, 80% of the surveyed companies reported that CS issues would have a serious negative impact on their business within a week of the issues happening, and 57% saying they would most likely become bankrupt or go out of business [5].

In an effort to mitigate against these threats, whilst being unable to afford costly enterprise-level security solutions, SMEs have tended to migrate their operations to the Cloud, in dramatically increasing numbers, even more so during the COVID-19 pandemic. A number of critical areas related to security and privacy viewed from both the *provider* and *end-user* perspectives can be summarized under governance (strategic and policy) and operations (architecture, tactical security and implementation) [6]. SMEs need to be aware of a number of key threats, challenges, risks and vulnerabilities of assets residing in the Cloud [7]. In order to raise SME's awareness to these challenges, analysing risks to their assets and preparing for improving their CS and PDP capabilities, the SCORE methodology seeks to provide answers to the following key questions dealing with (a) identifying current capabilities and assets, (b) analysing risks to these assets, (c) defining a future situation that ameliorates identified risks and (d) assessing the degree of satisfiability of a proposed transformation of capabilities.

III. Capability oriented RE

The notion of capability has been extensively researched in the field of strategic management, in which the main approaches are those of Resource Based View (RBV) [8] and Dynamic Capability Theory (DCT) [9]. In a capability-oriented paradigm we are interested in what has been identified in the strategic management field [10], as the possession of *valuable*, *rare*, *inimitable* and *non-substitutable*

[*] The work being presented in this paper has been partly funded by the European Union's Horizon 2020 Work Programme for research and innovation 2018-2020 under grant agreement n°101021659.

resources of enterprise as a source of sustainable advantage, whether these are existing capabilities or new ones that need to be introduced. Capability-orientation has attracted attention in a variety of fields including for example those of Information Systems [11] [12], Enterprise Architecture [13], Service Orientation [14], business/IT alignment [15] and digital transformation [16].

In the field of RE capability has been used as a suitable metaphor [17] providing the means of considering the intertwining of technical, organisational and social concerns in such a way, that it is possible to connect strategic objectives and high-level organizational requirements to technological artefacts in a unified manner [2]. The use of capability for representing the status of a business and its needs (the what) rather than focusing on the technical implementation (the how) serves as a powerful communication tool among business users and information technologists. Using capabilities as the starting point one can begin investigating and analysing what lies behind these fundamental enterprise assets, what goals govern them, what actors are involved and how they collaborate to synergistically meet requirements for enterprise transformation.

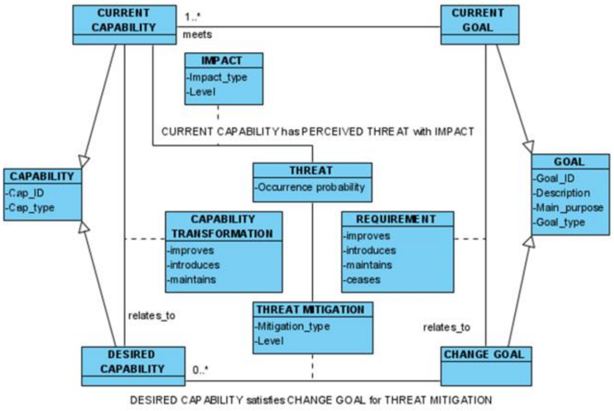

Fig. 1 SCORE core concepts

IV. THE SCORE APPROACH

The conceptual foundation of SCORE is provided by its metamodel, which at a high level of abstraction is shown in Fig. 1 which defines both CURRENT CAPABILITIES and DESIRED CAPABILITIES in order to model the necessary transformations from the former to the latter.

There is a symmetry between CURRENT CAPABILITIES and DESIRED CAPABILITIES in the sense that each set is related to enterprise goals, the former to CURRENT GOALS and the latter to CHANGE GOALS. Requirements are modelled and analysed in terms of the juxtaposition of CHANGE GOALS against CURRENT GOALS and their corresponding capabilities. In this sense SCORE incorporates the concept of *capability transformation* at the same time as considering *goals transformation*.

This metamodel is further detailed in Fig. 2. In terms of CS and PDP requirements the metamodel helps to record perceived THREATS that are identified by business users as having an IMPACT on CURRENT CAPABILITIES. Analysis of such threats and their potential impact will lead to the definition of new business goals (CHANGE GOALS) and their corresponding DESIRED CAPABILITIES leading to THREAT MITIGATION.

As shown in Fig. 2, a CAPABILITY is defined as an aggregation of PROCESSES using ASSETS. Threat mitigation is based on the implementation of appropriate organizational and technical measures (OTMs) pertaining to a DESIRED CAPABILITY aiming to protect the ASSETS being affected. For example, data breach is a THREAT that has a high impact on the organisation's capability to process personal data. Strengthening the current goal of secure data processing is of improve type REQUIREMENT that should be met by the desired personal data processing capability, which improves the current capability (CAPABILITY TRANSFORMATION) by implementing a number of OTMs such

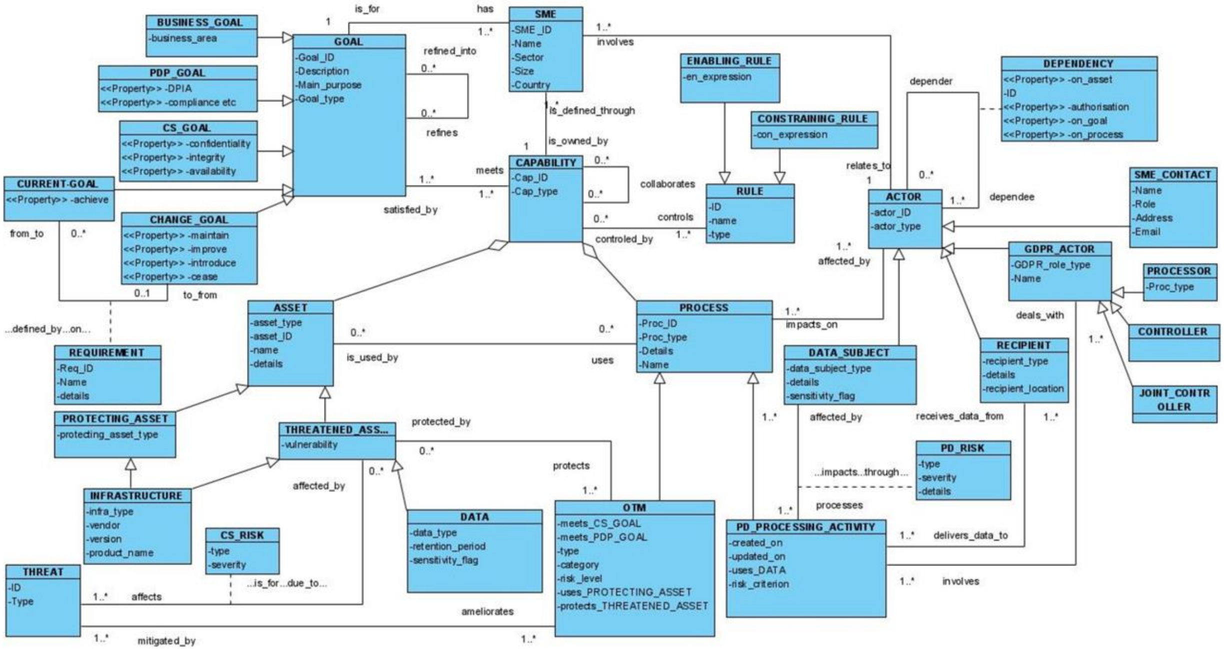

Fig. 2 Detailed SCORE concepts

as ‘enforcing an access control policy’, ‘authentication and access control’, etc., thus mitigating the THREAT.

In practice the conceptual modelling is considered along four viewpoints, namely those of: *capability*, *goal*, *actor-dependency* and *informational*. This allows stakeholders to focus their attention on specific aspects pertaining to their requirements and to also manage the complexity and volume of information being gathered, whilst conforming to the integrated conceptual framework. Given that these four modelling partitions are semantic projections on the single overall metamodel, it follows that the four individual viewpoints are **intrinsically interrelated** thus, when taken together, they present a holistic view of the situation being modelled. As demonstrated in section V there are anchor points in these viewpoints whose semantic relationships lead to ensuring completeness of all the different modelling views. These interrelationships objectively provide answers to the following questions: “*why does the enterprise need these capabilities?*” (answered by the *goal model*), “*what socio-technical actors are involved, how do they co-operate in order to realise these capabilities and how vulnerable to CS threats is this cooperation*?” (answered by the *actor dependency model*), “*what kind of information is used in this co-operation?*” (answered by the *informational object model*).

By ensuring that there are clear interrelations between the four different modelling views one is then able to (a) validate all models for consistency and completeness in a visual manner, (b) transition in a structured way from an existing set of capabilities to new desired ones for considering CS and PDP-related risks and (c) evaluate the risk mitigation proposition(s) in the desired situation.

The use of the SCORE methodology is effectively done using notations for each of the four modelling viewpoints as shown in Section V in which a use case is considered.

V. THE SCORE APPLICATION

SCORE has been applied on two in-depth pilot cases of SMEs for CS and PDP, one of which is considered in this section. Space limitations impose restrictions on a detailed exposition of all modelling nuances and on a full elaboration of the process followed. Nevertheless, two integrated models, one for the existing situation and the other for the desired one are shown such that they can assist in a reflective discussion about the utility of SCORE.

The SME involved owns 8 social care businesses, for which it processes and retains data about vulnerable people (its service users) for whom they have a duty to promote and maintain their welfare. The overall requirement of the SME is to have robust, fluid and dynamically changing CS systems that have the capacity to block threats and equally, to ensure that employees have the knowledge and skills required to avoid falling into ever-evolving security hazards.

Using appropriate questionnaires and meetings between SME personnel and requirements engineers, four modelling views were constructed corresponding to the current situation, dealing correspondingly with capabilities, goals, actors and data. Details of each separate type of model is beyond the scope of this paper but Fig. 3 shows fractions of these in inter-model relationships (based upon the details of the SCORE metamodel). The notations used are either new (in the case of capabilities) or extensions of notations used in goal-oriented RE and actor-dependency modelling [18], being partly assisted by an appropriate graphical tool [19].

The integrated model assists in focusing on specific questions to carry out risk analysis. Risk analysis aims to ascertain the current CS and PDP related risks, based on the identified threats noted in the capability model. In particular, the analysis is based on: (a) the occurrence probability of each threat which is calculated based on relevant vulnerabilities

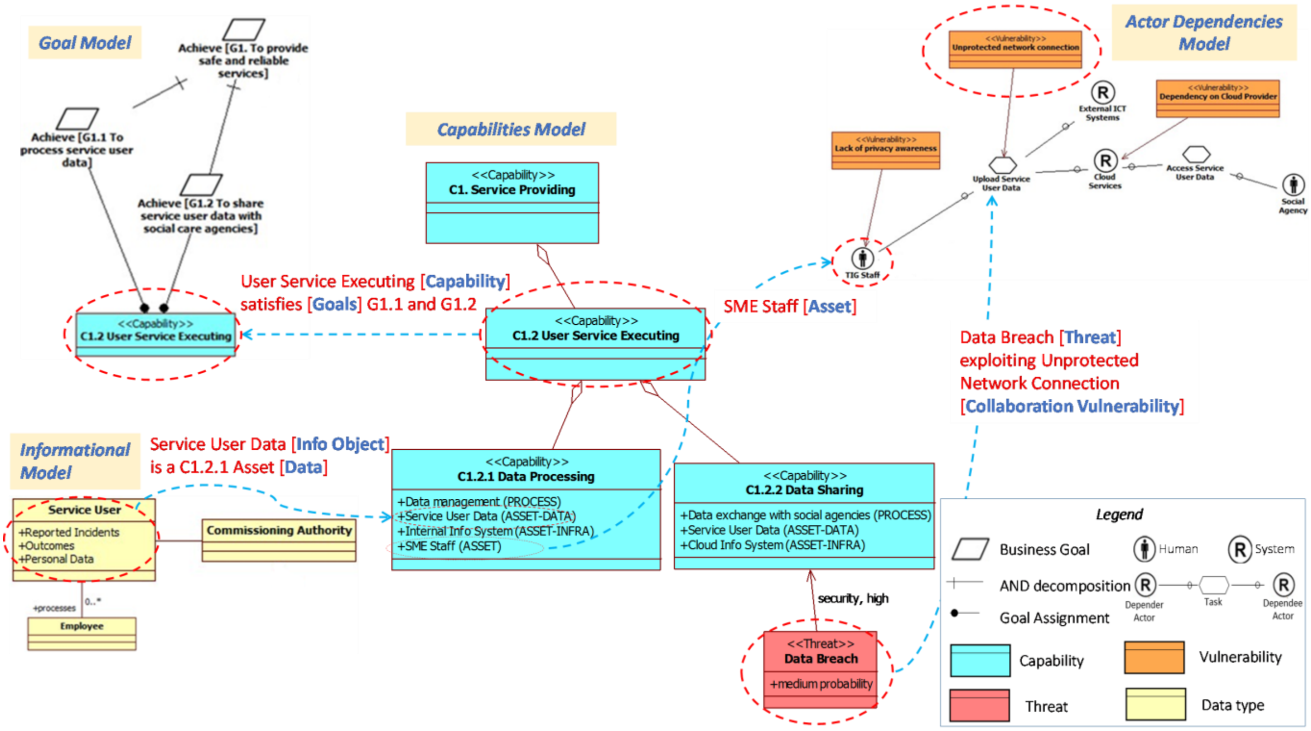
Goal Model
Achieve [G1. To provide safe and reliable services]
Achieve [G1.1 To process service user data]
Achieve [G1.2 To share service user data with social care agencies]
<<Capability>>
C1.2 User Service Executing
User Service Executing [Capability] satisfies [Goals] G1.1 and G1.2
Capabilities Model
<<Capability>>
C1. Service Providing
<<Capability>>
C1.2 User Service Executing
SME Staff [Asset]
Actor Dependencies Model
<<Vulnerability>>
Unprotected network connection
<<Vulnerability>>
Dependency on Cloud Provider
<<Vulnerability>>
Lack of privacy awareness
External ICT Systems
Upload Service User Data
Cloud Services
Access Service User Data
Social Agency
TIG Staff
Data Breach [Threat] exploiting Unprotected Network Connection [Collaboration Vulnerability]
Informational Model
Service User Data [Info Object] is a C1.2.1 Asset [Data]
Service User
+Reported Incidents
+Outcomes
+Personal Data
Commissioning Authority
+processes
0..*
Employee
<<Capability>>
C1.2.1 Data Processing
+Data management (PROCESS)
+Service User Data (ASSET-DATA)
+Internal Info System (ASSET-INFRA)
+SME Staff (ASSET)
<<Capability>>
C1.2.2 Data Sharing
+Data exchange with social agencies (PROCESS)
+Service User Data (ASSET-DATA)
+Cloud Info System (ASSET-INFRA)
security, high
<<Threat>>
Data Breach
+medium probability
Legend
Business Goal
Human
System
AND decomposition
Depender Actor
Task
Dependee Actor
Goal Assignment
Capability
Vulnerability
Threat
Data type

Fig. 3 Relationships between models of the current situation

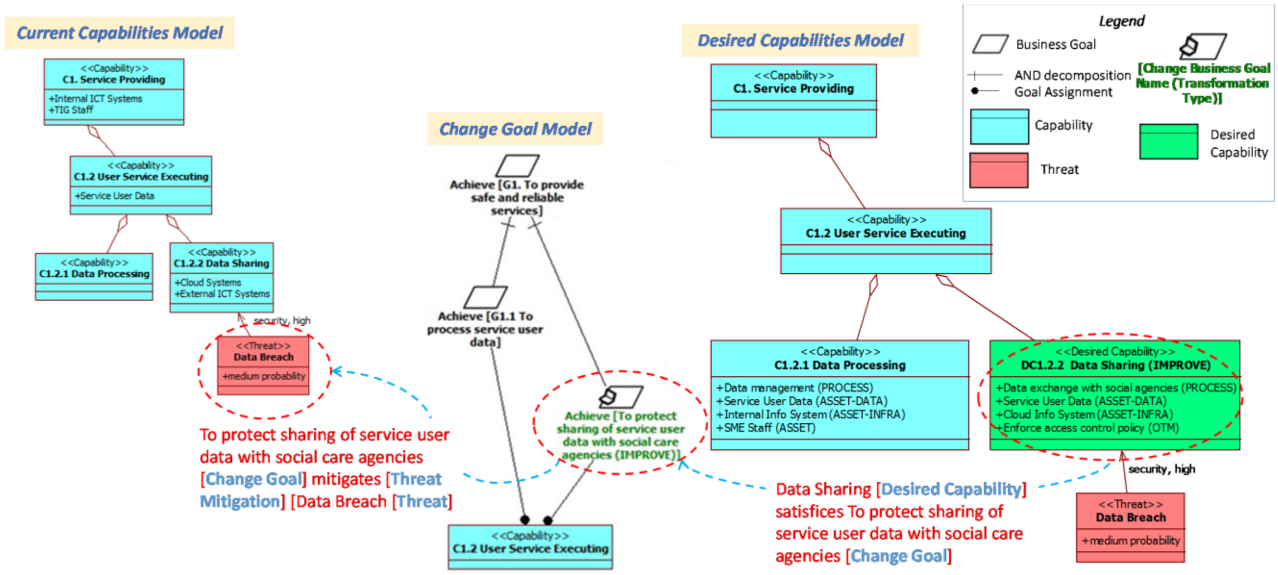
Current Capabilities Model
<<Capability>>
C1. Service Providing
+Internal ICT Systems
+TIG Staff
<<Capability>>
C1.2 User Service Executing
+Service User Data
<<Capability>>
C1.2.1 Data Processing
<<Capability>>
C1.2.2 Data Sharing
+Cloud Systems
+External ICT Systems
security, high
<<Threat>>
Data Breach
+medium probability
To protect sharing of service user data with social care agencies [Change Goal] mitigates [Threat Mitigation] [Data Breach [Threat]
Change Goal Model
Achieve [G1. To provide safe and reliable services]
Achieve [G1.1 To process service user data]
Achieve [To protect sharing of service user data with social care agencies (IMPROVE)]
<<Capability>>
C1.2 User Service Executing
Desired Capabilities Model
<<Capability>>
C1. Service Providing
<<Capability>>
C1.2 User Service Executing
<<Capability>>
C1.2.1 Data Processing
+Data management (PROCESS)
+Service User Data (ASSET-DATA)
+Internal Info System (ASSET-INFRA)
+SME Staff (ASSET)
<<Desired Capability>>
DC1.2.2 Data Sharing (IMPROVE)
+Data exchange with social agencies (PROCESS)
+Service User Data (ASSET-DATA)
+Cloud Info System (ASSET-INFRA)
+Enforce access control policy (OTM)
security, high
<<Threat>>
Data Breach
+medium probability
Data Sharing [Desired Capability] satisfices To protect sharing of service user data with social care agencies [Change Goal]
Legend
Business Goal
AND decomposition
Goal Assignment
Capability
Threat
[Change Business Goal Name (Transformation Type)]
Desired Capability

Fig. 4 Risk analysis – identifying desired capabilities

pertaining to related assets and their collaboration (described in the actor dependencies model), as well as the sensitivity of relevant data (described in the informational model); and (b) the level of impact of the threat (high, medium, low) on the affected capability (described in the capability model).

To demonstrate this, consider Fig. 3, which shows that the capability "C1.2.2 Data Sharing" is affected by the "Data Breach" threat. This threat exploits several vulnerabilities, as shown in the actor-dependency model. The "Service User Data" involved in the data sharing include personal and therefore sensitive data. Understanding such vulnerabilities is an important step towards risk analysis as it helps us to assess the likelihood and impact of the "Data Breach" threat. The occurrence probability of the "Data Breach" threat is medium while its impact on "C1.2.2 Data Sharing" capability is high and therefore triggers the need for change.

Risk analysis guides the identification of the new (change) goals to ameliorate the threat, which in turn guides the identification of the new (desired) capabilities to meet the change goals. By juxtaposing change goals on existing capabilities, in relation to the identified threat, it is then possible to define the new set of required capabilities. Again, detailed modelling is used for change goals and desired capabilities and Fig. 4 shows fragments of such models with their interrelations assisting in the definition of capabilities to ameliorate the threat of data breach.

Using the models, fragments of which are shown in Fig. 4, it is possible to evaluate to what degree the change goals may be satisfied. In particular, it involves the assessment of the type and level of mitigation for the perceived threat of the desired capability to satisfy the change goal. This type of analysis is guided by the semantic relationships between the different SCORE modelling concepts as shown in the example of Fig. 4. It can be observed that the desired capability "DC1.2.2 Data Sharing" improves the current data sharing capability by introducing the OTM "Enforce access control policy", thus satisfying the change goal of "To protect sharing of service user data with social care agencies". In this way, the desired capability provides a high level of response to the threat of "Data Breach", which may be subject to further evaluation by the SME management.

VI. Towards Tailor-Made Requirements Analyses

As mentioned in the introduction, the lack of resources in the form of both funds and in-house expertise is a dominant challenge in the SME landscape for CS and PDP. A key component in the process of addressing this challenge lies in the automation of the assessment process, which must precede the recommendation and deployment of the appropriate organisational and technical measures, or cybersecurity controls, for the protection of personal data. Self-assessment offers clear benefits by removing a part of the financial burden for external requirements engineers or for cybersecurity and GDPR consultants, thus helping SMEs focus on the PDP areas which matter most for their specific requirements.

Towards this end, SCORE offers specific RE enablers for self-assessment which can be leveraged by applications in the CS and PDP domain, through (a) an appropriate conceptual framework (detailed in section IV) for describing the knowledge related to the SMEs' requirements for CS and PDP, as well as for defining a common terminology for risk associated with the processing of personal data and for the required CS and PDP capabilities; and (b) a *pattern-driven approach* for self-assessment, whereby elicited knowledge about the SME requirements is used to recommend appropriate OTMs and other resources.

Patterns as a means to encapsulate and communicate proven security and privacy solutions, is an active and growing field of research [20-22]. In general they are architecture patterns that describe abstract building blocks or components (e.g., Safe Storage) that must be incorporated in the enterprise's security architecture in order to address certain security and privacy concerns (e.g., to mitigate a threat, to comply with a regulation or institutional policy, or to ensure some security or privacy property). They can also be considered as design patterns when they focus on implementation aspects of specific architecture components

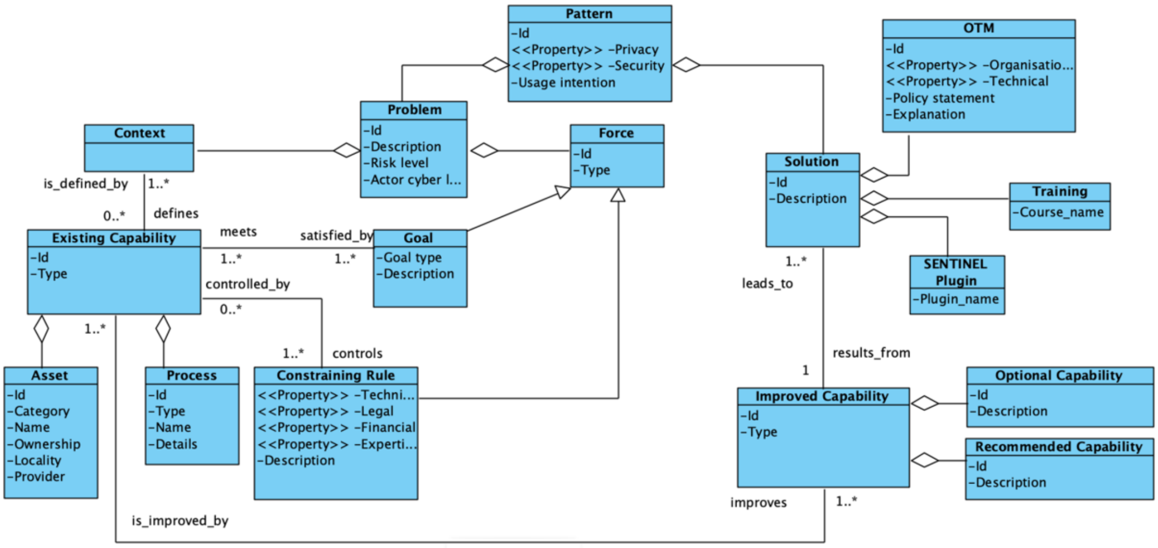

Fig. 5 The SCORE pattern conceptual model

(e.g., Hash Check as a Safe Storage implementation). Patterns can be generic or tailored to specific applications or architectural styles (e.g., web applications, IoT, cloud architectures, etc.). Existing pattern catalogues and online repositories are meant to assist IT architects and software developers to implement solutions that incorporate security and privacy by design, whilst in SCORE patterns are used in the context of the SME self-assessment as a means to assist SMEs to identify the appropriate OTMs that ought to be present in their CS and PDP policy. Patterns are described in terms of the relevant concepts defined at a conceptual level in SCORE, as shown in the pattern's conceptual model in Fig. 5. In more detail, a `Pattern` is composed of its two basic structural elements namely those of `Problem` and `Solution`. The `Problem` itself is defined in terms of its `Context` and `Force(s)`.

For the `Context` we are interested in defining the business setting of an SME. In particular, a `Context` can be defined in terms of the SME `Existing Capability` that can be made very specific in terms of two concepts of interest to self-assessment namely those of `Asset` and `Process`. In the pilot case presented in section V, this would be having the existing capability of "`Service Providing`", which is further specified in terms of the "`Data sharing with social agencies`" process, which uses two assets namely those of "`Service User Data`" and "`Cloud Information System`".

For the `Force` we are interested in those elements that influence the `Problem` and which must be resolved. In our modelling these would be the `Goal` and the `Constraining Rule`, both of which are related to the `Existing Capability`. In our example these would be the SME goal of "`improving the protection of service user data`", and legal constraint of "`conforming to government regulations`".

The second main element of the template is that of the Solution. The `Solution` is made up of three elements namely those of policies (`OTM`), awareness practices (`Training`) and technology components (`Software Plugin`). Applying the `Solution` would lead to some `Improved Capability`, defined in terms of `Recommended Capability` and `Optional Capability`.

The data related to the `Problem` are instantiated values of the SCORE concepts provided by the SME users, using appropriate questionnaires, whilst the `Solution` is informed by a) the hierarchy of the ISO/IEC 27001:2013 standard [23] and b) ENISA's risk-based approach to protecting personal data [4, 24].

In the pilot case the recommended OTMs forming the solution include "`To enforce access control policy`" and "`To provide third-party delivered and monitored CS services`".

Depending on how generic is the definition of the pattern it could be useful in similar businesses or any other company in the service sector. It is then up to the scheme of how one may identify applicable patterns in different domains. This can be achieved in terms of a pattern language such as the one shown in Fig. 6. Considering the pilot case of section V, we can define an instance of the above rule as shown in Fig. 7.

```
If there exists a Context defined by
  an Existing Capability $C_i$
      involving Assets $A_1$, .. $A_n$
      AND Processing Activities $PA_1$, ..,$PA_n$
  with Problem of
      Risk Level $RL_i$
      AND Actor Cyber Level $ACL_i$ identified by
        a set of Forces
          involving Goals $G_1$, $G_2$, ..$G_n$
          AND/OR Constraining Rules $R_1$, $R_2$, ..,$R_n$
Then apply Solution $S_i$
  involving $OTM_i$ AND/OR $TRAINING_i$ AND/OR $PLUGIN_i$ that
        improve Goals $G_1$, $G_2$, ..$G_n$
        AND/OR meet Constraining Rules $R_1$, $R_2$, ..,$R_n$
  leading to Recommended Capability $RC_i$
        AND Optional Capabilities $OC_1$, $OC_2$, ...$OC_n$
```

Fig. 6 Rule-based description of the pattern template

Using the pattern template and the pattetrn language one is able to generate, maintain and reuse a knowledge base appropriate for analysis of CS and PDP requirements in a given domain without the need for financial impositions for appropriate experstise and costly software solutions. Towards

```
If there exists a Context defined by
  an Existing Capability Service Providing
    involving   Assets   Cloud   IS   (sw_saas,   cloud,
no_owned_asets, google)
    AND Processing Activities Data exchange with social
agencies
  with Problem of Risk Level risk high
    AND Actor Cyber Level intermediate identified by
      a set of Forces
      involving  Goals  Confidentiality  of  service  user
data
      AND/OR Constraining Rules CQC/CIW Regulations
Then apply Solution Si
  involving O1.H.1 (Semester PDP Policy Review Process)
    that  meet Constraining Rules CQC/CIW Regulations
    AND improve Goal Confidentiality of service user data
  leading      to      Recommended      Capability      O1
(org_policy_drafting_enforcing, Defining and enforcing
a policy)
    AND Optional Capability s_cloud_security (To provide
                third-party     (Cloud)-delivered     and
                monitored CS services)
```

Fig. 7 Example instance of the pattern template

this end, work is under way towards the development of an innovative platform for providing such capabilities for SMEs in a wide variety of business sectors.

VII. Conclusion

Data breaches cause massive losses to organizations. Smaller enterprises often do not possess advanced CS solutions to cope with an evolving threats landscape. Free security options provide rudimentary protection at the endpoint level but leave what matters most for customers, sensitive personal data residing in web apps and other infrastructures, exposed. In the RE literature there are a number of methodologies that attempt, in a variety of ways, to deal with the capture, analysis, and specification of user requirements relating to CS for privacy. In *risk-oriented* RE, attention is given to the protection of assets through the treatment of threats that put information at risk. In *goal-oriented* RE, emphasis is given on non-functional requirements. The advent of Cloud computing requires of SMEs to identify the appropriate services offered by external providers. This raises the need for a new RE metaphor that will enable the mapping of business security requirements onto external or internal service provision through appropriate capabilities. SCORE, by paying particular attention to advancing a user-centric viewpoint, offers a clear methodology for SME stakeholders to engage in their articulation, representation and analysis of their requirements for CS and PDP, driven by a capability oriented 'philosophy'. SCORE also offers opportunities for the automation of assessing the degree of maturity in an SME's capability handling of its CS and PDP challenges [25].

Acknowledgment

We are indebted to Daryl Holkham of Tristone Investment Group (TIG) for his assistance in the elicitation of their company requirements (section V) and more generally to SENTINEL colleagues for useful discussions regarding the ongoing project work.

References

1. Benz, M. and D. Chatterjee, *Calculated risk? A cybersecurity evaluation tool for SMEs.* Business Horizons, 2020. **63**(4): p. 531-540.
2. Loucopoulos, P., E. Kavakli, and J. Mascolo, *Requirements Engineering for Cyber Physical Production Systems: The e-CORE approach and its application.* Information Systems, 2022. **104**(Feb. 2022).
3. ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises*. 2015, European Union Agency for Network and Information Security.
4. ENISA, *Guidelines for SMEs on the security of personal data processing*. 2016, European Union Agency for Network and Information Security.
5. ENISA, *Cybersecurity for SMEs: Challenges and Recommendation*. 2021, European Union Agency for Cybersecurity.
6. Cloud Security Alliance (CSA). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. 2017 30th July 2021]; Available from: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.
7. Cloud Security Alliance (CSA), *Top Threats to Cloud Computing: The Egregious 11*. 2019, Cloud Security Alliance.
8. Helfat, C.E. and M.A. Peteraf, *The dynamic resource-based view: capability lifecycles.* Strategic Management Journal, 2003. **24**(997-1010).
9. Teece, D.J., *Dynamic Capabilities and Strategic Management*. 2009, United States, New York: Oxford University Press.
10. Barney, J., *Firm Resources and Sustained Competitive Advantage.* Journal of Management, 1991. **17**: p. 99-120.
11. Liang, T.-P. and J.J. You. *Resource-based View in Information Systems Research: A Meta-Analysis*. in *Pacific Asia Conference on Information Systems (PACIS)*. 2009.
12. Danesh, M.H. and E. Yu, *Modeling Dynamic Capabilities to Reason about Information Systems Flexibility*, in *CAiSE 2014 (Submitted)*. 2014.
13. Iacob, M.-E., D. Quartel, and H. Jonkers, *Capturing Business Strategy and Value in Enterprise Architecture to Support Portfolio Valuation*, in *16th International Enterprise Distributed Object Computing Conference (EDOC 2012)*. 2012, IEEE: Beijing, China. p. 11-20.
14. Homann, U., *A Business-Oriented Foundation for Service Orientation*. 2006, Microsoft Developer Network.
15. Bērziša, S., et al., *Capability Driven Development: an Approach to Designing Digital Enterprises.* Business & Information Systems Engineering, 2015. **57**(1): p. 15-25.
16. Danesh, M., P. Loucopoulos, and E. Yu, *Dynamic Capability for Sustainable Enterprise IT: A Modelling Framework*. 2015: 34th International Conference on Conceptual Modeling (ER 2015).
17. Cao, J., et al. *Capability as Requirement Metaphor*. in *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. 2011.
18. Dalpiaz, F., X. Franch, and J. Horkoff, *iStar 2.0 Language Guide*. 2016.
19. Supakkul, S. and L. Chung. *RE-Tools: A Multi-notational Modelling Toolkit*. 2009-2012 1st July 2021]; Available from: http://www.utdallas.edu/~supakkul/tools/RE-Tools/index.html.
20. Papoutsakis, M., et al., *Towards a Collection of Security and Privacy Patterns.* Applied Sciences, 2021(11).
21. Vale, A.P. and E.B. Fernandez, *An Ontology for Security Patterns*, in *38th International Conference of the Chilean Computer Science Society (SCCC)*. 2019, IEEE: 38th International Conference of the Chilean Computer Science Society (SCCC).
22. Washizaki, H., *Security patterns: Research direction, metamodel, application and verification*, in *2017 International Workshop on Big Data and Information Security (IWBIS)*, IEEE, Editor. 2017: Jakarta, Indonesia. p. 1-4.
23. ISO/IEC, *Information technology — Security techniques — Information security management systems — Requirements*. 2013, International Standards Organisation.
24. ENISA, *Handbook on Security of Personal Data Processing*. 2017, European Union Agency For Network and Information Security.
25. Grabis, J.n., J. Stirna, and J. Zdravkovic. *Capability Management in Resilient ICT Supply Chain Ecosystems*. in *22nd International Conference on Enterprise Information Systems (ICEIS 2020)*. 2020.