# Capturing strategic competences: cloud security as a case study

Mingtao Shi

Mingtao Shi is based at the Department of Research & Development, Innovation and Intellectual Property, Francotyp-Postalia Group, Birkenwerder, Berlin, Germany.

## 1. Introduction: resource-based strategy

Strategy at the business level aims at individual business units within a corporation. Two schools of thought have become the major focus of the debates on the subject of business strategy both in academia and among practitioners. The ''outside-in perspective'' suggests that the environment around the firm is the key to profitability and the organisation should adapt itself to the market position envisioned, while the ''inside-out perspective'', also called the ''resource-based view'' (RBV), on the contrary, looks inwardly into the firm and consists of managers who believe that competition eventually takes place around a firm's resource bases and that strategies fostering unique resources are fundamental for sustained competitive advantages (de Wit and Meyer, 2010).

Published qualitative and quantitative research papers over the past two decades have gradually strengthened the empirical basis of the RBV (see, for example, Collis and Montgomery, 1991; Maijoor and van Witteloostuijn, 1996; Majumdar, 1998; Makhija, 2003). According to the RBV, the resources of a firm must possess a number of characteristics in order to be strategic. Strategy writers have constructed models to describe such properties. An influential framework is the VRIO model, which advances a number of sufficient preconditions for resources to gain sustained competitive advantage (Barney, 1991, 2002):

- Value – Resources are valuable when they enable a firm to perform higher efficiency and effectiveness in operational activities.
- Rareness – The same value-creating resources are not possessed by other competitors.
- Inimitability – Firm resources are difficult to be duplicated or substituted and resources can become imperfectly imitable for one or a combination of three reasons: the ability of a firm to obtain a resource is dependent upon unique historical conditions; the logical link between the resources possessed by a firm and a firm's sustained competitive advantage is causally ambiguous; or the resource generating advantage is socially complex.
- Organisation – How the firm is structured, organised and managed to exploit valuable, rare and costly-to-imitate resources.

Three developmental trends have been identifiable within the inside-out perspective:

1. the traditional school of RBV, which is composed of authors who have coined terms such as ''resources'', ''dynamic capabilities'' and ''core competences'' and have emphasised the usefulness of organisational assets in generating superior firm performance;
2. the knowledge-based view (KBV), contending the decisive role that collective and individual knowledge plays; and
3. the relational view, arguing the economic advantages of inter-firm relations (Acedo *et al.*, 2006).

DOI 10.1108/JBS-01-2013-0004

The term ''strategic competences'' is defined more broadly in this paper as organisational resources that are either of a material or an immaterial nature and can contribute to the successful accomplishment of a firm's productive activities.

Although the inside-out perspective has evolved significantly, how strategic competences are identified remains inadequately discussed in the published studies. The body of knowledge in this area, however, is importantly relevant for the further development of the theory and for business managers in the field. This paper intends to develop a concept that can lead to the recognition of a firm's strategic competences on the one hand and attempts to suggest some general patterns of action to treat identified competences on the other.

## 2. Approach: cloud security as a case study

Information security in cloud computing (henceforth ''cloud security'') is used as a case study to introduce the concept of capturing strategic competences. Information technology (IT) has become increasingly ubiquitous for businesses (Sosinsky, 2011; Baun *et al.*, 2010). Today, with few exceptions, firms are replying heavily upon competences related to IT in order to deliver outputs for their respective product markets. A number of competence sets that were rare five to ten years ago have become basic skills in many businesses. Resources related to networking, applications embedded in value chain activities and e-commerce are valuable, but do not confer durable advantages on firms any more. Clearly, as a part of the competence base is eroding, new strategic competences must be gained for businesses to stay competitive. In many cases, it is not the applications and technologies themselves but their security issues that have increasingly received firms' attention (Turban and Volonino, 2010). Cloud applications are especially exposed to security vulnerabilities because of their comprehensive use of network and web technologies. Since clouds have become particularly widely used in recent years, cloud security is one major competence area for many businesses to achieve IT-based advantages. The literature in this area has emerged recently. Many sources describe the specific threats in the cloud and suggest means to prevent and tackle malicious attacks (see, for example, Terplan and Voigt, 2011; Winkler, 2011; Krutz and Vines, 2010; Mather *et al.*, 2009). Few, however, have looked at cloud security from the perspective of developing strategy.

The author of this paper has gained expertise in cloud security by directing consultancy teams in a number of relevant projects. The case study presented in this paper therefore uses results that are based upon project data stemming from firms operating in the health, banking and telecommunications industries. The names of the businesses are anonymised because of non-disclosure settlements agreed among the actors. The main objective of the projects was to advise firms on finding the necessary skills to tighten their respective cloud environments in terms of information security.

## 3. Strategic competences in cloud security

Competences that are of strategic importance are different in different functional contexts. The unit of analysis in this paper focuses on the ''competence domains'' that perform tasks, deliver results and create value within or across the functional departments of a business. In a financial department, for example, knowledge of accounting practices, the procedures defined for internal audits, and the routines developed for the assessment of currency risk are such competence domains, in which strategic competences may reside. The technique developed in this article may serve as a general analytical tool to capture strategic competences and may be applied to any businesses or functional areas within a particular business.

By responding to enquiries and tenders and investigating circumstances surrounding the cloud in various contextual environments, it was found that an effective beginning point for capturing strategic competences is to elicit data. A number of methods of investigation, such as creativity techniques, observation, interviews and questionnaires, may support the elicitation process effectively. Firms troubled by security problem suffer from different types of external threats, such as eavesdropping, theft, sabotage and fraud. These threats are

materialised in security attacks. Logon abuse, wireless local area network (WLAN) eavesdropping, network intrusion, denial of service (DoS), spoofing, man-in-the-middle, social engineering, dumpster diving, password guessing and malware are the most widespread forms of attack that can significantly deteriorate cloud security. The high complexity of the technology also causes vulnerabilities within the cloud itself. Virtualisation technology, application configuration and the management of access rights are examples of such internal security concerns. Data elicitation in general contributes to identifying security problems and possibly the sources of these problems, which forms an important basis for approaching the nature and defining the scope of the competence domain concerned. The insights acquired can be registered in an information pool, for example in the form of a list. After the threats are localised, it is certainly necessary that individual mechanisms encountering and solving the internal and external security problems are provided. Mastering the solutions to individual problems epitomises the competence set that may potentially generate competitive advantages for the firm.

The solutions dealing with the individual attacks and vulnerabilities can be gathered in another column of the same list, just next to the questions and problems identified. Project experience shows that, as a next step, it may be useful to categorise the solutions in multiple dimensions. In the case of cloud security, individual solutions generated can be ordered as either managerial, or legal or technological countermeasures. Systemising solution methods into a few categories may help managers maintain a clear overview of the broader fields of expertise for further analysis. A strategic competence does not mean to solely possess a piece of information or to be able to apply the information to the operational environment. Strategic competences are rather a firm's learning capabilities similar to the ''double-loop learning'' advocated by Argyris (1977). In the case of cloud security, for example, one countermeasure to WLAN eavesdropping is to deploy a cryptographic key, which encrypts the information on the communication paths. Another safeguard against eavesdropping is to install WLAN management systems that can detect and track attacking devices. While owning this kind of information or knowledge is necessary to solve individual problems, managers need to formulate the implications of such knowledge to a firm's competences. A cryptographic key or management systems as software applications are operational measures. Managers should rather ask themselves questions such as ''How can we build a safer communication platform for all electronic devices such as computers, notebook, routers, servers, and mobile phones?''. The answer to this question may become the formulation of a potential competence: ''We need to build an encrypted communication environment while dealing with cloud applications and a key infrastructure to protect the devices and information exchanged between them''. Similarly, information about management applications against WLAN eavesdropping may lead to the consideration: ''Security software packages such as WLAN management system, intrusion detection system (IDS) and anti-malware software are of general interest. We should be well informed about the significant software tools related to information security in the market and own in-depth technical knowledge that enables the security staff to install, configure, maintain and update the tools on different types of devices that are connected to the cloud''.

Figure 1 shows how the steps ''Elicit-Solve-Categorise-Formulate'' discussed above are applied in the case of cloud security. It illustrates the essential steps for capturing the strategic competences rather than listing exhaustively all security concerns and solutions found during the conduction of the projects.

The process of capturing strategic competences essentially involves looking through the mysterious veil of the phenomena in business operations to unveil the nature of the mundane problems and thereby form a sound basis for strategic management decisions. In order to achieve the best possible results during this process, two groups of participants are especially expected to co-operate with each other closely. The domain specialists are obviously the knowledge carriers and play a decisive role in delineating, analysing, benchmarking and evaluating competences. The process in one competence domain may certainly also involve knowledge providers of other relevant competence domains. The project findings of cloud security presented in this paper are the results of joint efforts made

**Figure 1** ''Elicit-Solve-Categorise-Formulate'': deriving competence implications in cloud security

| ① Elicit<br>***Attacks & Vulnerabilities*** | ② Solve<br>***Security measures***<br>③ Categorise | ***Competence implications***<br>④ Formulate |
|---|---|---|
| **Category: Managerial aspects** | | |
| Logon abuse | Defining fine-grained access rights for cloud applications | *Identity and Access Management (IAM)* |
| Social engineering; dumpster diving | Treating phishing attempts effectively and nurturing behavioural awareness towards information exposure | *Security awareness*: creating internal security team with certified members (certifications such as CISA, CISM, and CISSP); organising training and educational programmes; involving top management |
| Password guessing | Strengthening the length and complexity of passwords | *Security guideline*: instructing the rules and change frequency of passwords |
| Unforeseeable system outage caused by human, organisational, technical or natural reasons | Developing emergency plans based upon the structure of information objects | *Business Impact Analysis* (BIA); *Disaster Recovery Plan* (DRP) & *Business Continuity Plan* (BCP); *Risk management* (recognition of possible negative events that may take place in the cloud and their probability, evaluation of impacts, preparation and deployment of proven measures to reduce, transfer or avoid these risks) |
| Shared clipboard; keystroke logging; rogue hypervisor; virtual machine monitoring | Implementing security measures such as securing root; hardening hypervisor, virtual machines and the host; regular data backup; installing security patches and updates | *Virtualisation management* (managerial and technical activities around the issues that arise because of the virtualised environment in the cloud); *Risk* management; *Security guideline*: introducing backup, patch & update standards |
| **Category: Technological aspects** | | |
| WLAN Eavesdropping | Deploying cryptography; installing WLAN management system | *Public Key Infrastructure (PKI); security software systems; configuration management (security software)* |
| Network intrusion | Making use of Intrusion Detection System (IDS) | Selecting and implementing *security software systems; configuration management (security software)* |
| Denial of service | Applying blacklist, firewall filtering and routers with limitation functionalities | *Security guideline*: setting rules for the configuration; *configuration management* (technical instances involved in the cloud) |
| Spoofing | Applying gateways and packet filtering | |
| Man-in-the-Middle | Enabling secured communication paths; deploying cryptography and certificates during the communication; applying mTAN (mobile Transaction Authentication Number) for important monetary transactions | *Virtual Private Network (VPN)*; *SSL* (Secure Sockets Layer); *IAM; PKI* |
| Malware | Selecting and installing anti-malware tools; establishing guideline | *Security software systems*; *security guideline*: stipulating rules for update and incident procedures; *DRP* |
| **Category: Legal aspects** | | |
| Treatment of application and recruitment data | Conceptualising standards for receiving, forwarding and deleting applicants' personal data, based upon the principles of privacy protection | Competence in *national or sectoral regulations*, in Germany for example: German Federal Data Protection Law (BDSG), Telecommunications Law (TKG), Telemedia Law (TMG); *Security awareness*: creating internal legal team specialised and certified in information security |
| Data processing through a third party | Integrating contractual rules for transferring, storing, processing personal and commercial data by the third party and for destroying data upon the termination of the contract | |
| Access to rooms and systems with sensitive information | Creating fine-grained rights for accessing physical facilities and electronic systems (password, token, card, biometric) | |
| Lawful compliance | Establishing the role "supervisor for data protection", a directory that documents how data elements are processed in different internal processes; enabling ex-ante control mechanisms verifying the lawfulness of the planed data gathering and processing procedures | |

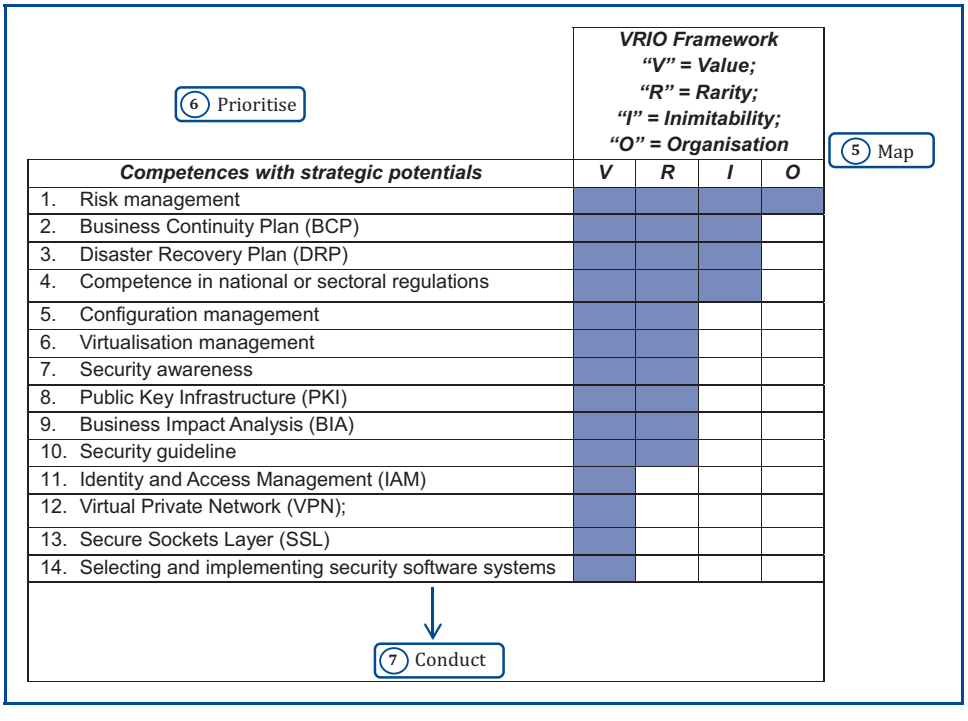
not only by the cloud security team, but also by adjacent or other competence domains such as application development, infrastructure administration and the functional managers responsible for the important cloud applications used by the investigated firms. Strategy managers are typically central instances within a strategic business unit, contributing to the communication, organisation and documentation of the process through all the steps described above.

When the competences are made visible by the derived implications, it is necessary that they are mapped against the VRIO framework. The next step for capturing strategic competences thus focuses upon testing the strategic meaning of the competences. During this step, the actors may ask themselves if each of the extracted competences possesses the potential to be valuable, rare, and inimitable and is properly exploited by the existing organisational structure of the firm. Clearly, benchmarking must be performed in this kind of dissection. It is essential that especially the domain specialists should be capable of understanding and comparing the relative performance of the concerned competence domain *vis-à-vis* the firm's competitors. The mapping analysis can be carried out in a qualitative manner and its results should also be documented for further analysis. Either ''yes'' or ''no'' as an answer to the criteria of the VRIO framework may leave room for interpretation during the strategic analysis, but can simplify the strategic process beneficially. Quantification of the variables may turn out to be time-consuming and impracticable for daily businesses.

Once the mapping is completed, a further analysis step should prioritise the competences in a sorted order that places the competences that have the greatest fit to the VRIO criteria at the top of the list. The strategist can enlist the insight gained during the prioritisation step to embark on competences according to their strategic importance. Figure 2 demonstrates how the steps ''Map'' and ''Prioritise'' can appropriately capture the competences of strategic importance in the case of cloud security. The shaded fields imply a ''yes'' answer during the mapping step.

Once the strategic meaning of the competences is deciphered, the final step is to choose a pattern of conduct according to the importance of the respective competences. During this

**Figure 2** ''Map-Prioritise'': capturing strategic competences in cloud security



step, strategy managers become ultimately responsible for recommending the possible patterns of action that are needed to improve the performance of the competence domain involved. Strategy managers may also contribute considerably to the tactical implementation of the chosen actions by acquiring and coordinating hardware, software, human-ware, and organisation-ware. Discussions carried out in the projects related to cloud security revealed that two dimensions may be vital when managers design the patterns of action. Managers should be aware if and to which extend the captured competences are already available in the organisation. A way to gain a relatively precise impression of the stock level of a competence is to scale the existence of the competences in ''not available'', ''low'', ''medium'' and ''high''. The second dimension is the strategic fit of the competences to the VRIO model found during the previous steps. Both dimensions jointly influence the manager's decision on what should be conducted. One possible set of the action patterns is suggested as follows:

1. If a competence is not valuable or not valuable any more, managers should immediately divest this competence, release and reallocate the underlying resources occupied by it.
2. If a competence is valuable, it can only generate parity performance *vis-à-vis* a firm's competitors:
   - (Stock level of this competence is ...) ''not available'' or ''low'': managers should allocate resources and budgets; define time frame, goals and expected results; fostering learning by doing (single-loop learning) to build this competence.
   - ''Available'' (low, medium and high): manager should maintain the productive activities enabled by this competence and should not pursue cost-intensive and time-consuming investments to further develop this competence.
   - ''Selecting and implementing security software systems'' is such a competence in the case of cloud security (see Figure 2).
3. If a competence is valuable and rare, it can bring about temporary competitive advantage:
   - ''Not available'' or ''low'': managers should organise to add stock to this competence, by investing time, financial and other types of resources moderately.
   - ''Medium'' or ''high'': it is likely that this competence has contributed greatly to the competitiveness of the competence domain involved in the past, but now begins to erode in terms of inimitability. Two possibilities are existent in this case. If the competence still possesses a reasonable potential to become strategic again, by allocating resources and budgets, managers should replenish the competence, in order to enhance or modify the structure of the competence, which aims at inimitability. Sources of the inimitability usually reside in history and social complexity within and surrounding a firm. However, if the evaluated potential for this competence to become strategic again is rather pessimistic, it should be gradually replaced. Managers should then strive to build and nurture other types of competences that produce the same services and results.
   - Being capable of designing and conducting ''business impact analysis'' is, for example, such a competence in the case of cloud security.
4. If a competence is valuable, rare, hard to imitate or even simultaneously well absorbed by the existing organisational structure of the firm, it undoubtedly contributes to sustained competitive advantage:
   - ''Not available'' or ''low'': managers should quickly allocate resources and budgets; define time frame, goals and expected results; foster learning by doing (single-loop learning) to accelerate the emergence or further development of this competence.
   - ''Medium'': managers should heavily reinforce the resources and budgets connected with this competence; define further time frame, goals and expected results; introduce the concept of ''learn how to learn'' (double-loop learning). The additional investments should seek higher scales economies and improved quality of the produced results.

- ''High'': managers should exploit and harness this competence fully to generate durable advantages. The achieved scales economies due to the high stock of the competence may enable the managers to release partial resources linked to this competence. The released resources should ideally be reserved for achieving a higher durability of this strategic competence.
- A firm's capability to perform high-quality ''risk management'' or ''business continuity plan'' is such a competence in the case of cloud security.

5. If the value of a competence is still unknown or uncertain: no immediate action is required. Managers should further evaluate this competence and conduct feasibility study, in order to observe the necessity of building or adding stock to this competence.

## 4. Conclusion: capturing strategic competences

This paper introduces a concept of capturing strategic competences within a firm. The theoretical foundation lies in the resource-based view, a major school of thinking in the field of business strategy. The VRIO model within this school contends that competences that generate sustained competitive advantage are simultaneously valuable, rare, costly to imitate and fit the existing organisational structure of the firm. It is assumed in this paper that a strategic business unit consists of different functional departments, each of which is composed of a number of competence domains. The task of the strategic management is to first capture and then to build or strengthen the strategic competences in individual competence domains, which in turn may effectuate, tighten and prolong the overall competitive advantages of a firm.

Cloud security is selected to accompany the description of the concept. The case study shows that strategic competences can be effectively recognised following the steps: ''elicit-solve-categorise-formulate-map-prioritise-conduct''. This instrument of analysis can interpret the issues and problems in daily business, abstract to find competence implications, relate the findings to the VRIO model and finally derive strategic competences. Managers and scholars can use the framework provided to shed light on potential competences that can significantly impact a firm's economic performance. Furthermore, this paper also suggests a set of operational patterns to treat the competences according to their strategic importance. Managers can design implementation approaches to either accelerate the emergence of, or reinforce, or exploit competences of high strategic meaning. Additional stock is added to the moderately important competences or theses competences are replenished or replaced. Competences that are of value only are either built or should be maintained at the same stock level. Competences of less meaning should be either divested or observed for further action.

## 5. Study limitations and further research

Developing a concept with a higher generalisability must enlist support from more than just one case study. A case study may depict the model exemplarily, but further studies in other competence domains, functional areas, firms and industries must be carried out. Further studies may also explore the linkages among competence domains and functional areas in order to illuminate how inter-departmental and inter-domain competences can enable more efficient and effective interactions. Furthermore, the mapping to the VRIO model in this paper is based upon a qualitative approach with a ''yes'' or ''no'' assessment. Future investigations may discuss whether a quantitative methodology without significantly more time and resource expense may be necessary to enhance the precision of the concept.

*Keywords:*
Strategic competences,
Resource-based view,
Resources,
Competence domains,
Cloud security,
Cloud computing,
Competences

## References

Acedo, F.J., Barroso, C. and Galan, J.L. (2006), ''The resource-based theory: dissemination and main trends'', *Strategic Management Journal*, Vol. 27 No. 7, pp. 621-636.

Argyris, C. (1977), ''Double-loop learning in organizations'', *Harvard Business Review*, Vol. 55 No. 5, pp. 115-125.

Barney, J. (1991), ''Firm resources and sustained competitive advantage'', *Journal of Management*, Vol. 17 No. 1, pp. 99-120.

Barney, J. (2002), *Gaining and Sustaining Competitive Advantage*, 2nd ed., Prentice Hall, Upper Saddle River, NJ.

Baun, C., Kunze, M., Nimis, J. and Tai, S. (2010), *Cloud Computing: Web-basierte dynamische IT-Services*, Springer, Berlin.

Collis, D.J. and Montgomery, C.A. (1995), ''Competing on resources: strategy in the 1990s'', *Harvard Business Review*, Vol. 73 No. 4, pp. 118-128.

de Wit, B. and Meyer, R. (2010), *Strategy: Process, Content, Context*, 4th ed., Cengage Learning EMEA, Andover.

Krutz, B.L. and Vines, R.D. (2010), *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*, Wiley, Indianapolis, IN.

Maijoor, S. and van Witteloostuijn, A. (1996), ''An empirical test of the resource-based theory: strategic regulation in the Dutch audit industry'', *Strategic Management Journal*, Vol. 17 No. 7, pp. 549-569.

Majumdar, S.K. (1998), ''On the utilization of resources: perspectives from the US telecommunications industry'', *Strategic Management Journal*, Vol. 19 No. 9, pp. 809-831.

Makhija, M. (2003), ''Comparing the resource-based and market-based views of the firm: empirical evidence form Czech privatisation'', *Strategic Management Journal*, Vol. 24 No. 5, pp. 433-451.

Mather, T., Kumaraswamy, S. and Latif, S. (2009), *Cloud Security and Privacy*, O'Reilly Media, Sebastopol, CA.

Sosinsky, B. (2011), *Cloud Computing Bible*, Wiley, Indianapolis, IN.

Terplan, K. and Voigt, C. (2011), *Cloud Computing*, MITP, Heidelberg.

Turban, E. and Volonino, L. (2010), *Information Technology for Management*, Wiley, Hoboken, NJ.

Winkler, V.J.R. (2011), *Cloud Computer Security Techniques and Tactics*, Elsevier, Boston, MA.

## About the author

Mingtao Shi is currently Senior Technical Product Manager at the global headquarters of Francotyp-Postalia Group in Germany and has worked in the ICT industry for over ten years. He received a PhD from Technische Universität Berlin in 2007. Since then, he has been a part-time lecturer at several universities and an active researcher, focusing on strategic and innovation management. He has published a monograph and a number of peer-reviewed journal articles, and is an editorial board member of the journal *Computer and Information Science*. Mingtao Shi can be contacted at: c.shi@francotyp.com