19
DIGITAL CAPABILITY
Scaffolding for rewiring a company for digital
Joe Peppard

Introduction
In recent years, the label of digital has entered the lexicon of management and in many organizations digital has now become a fashionable rallying cry. Digital is simultaneously a technology, an objective, a threat, an opportunity, a workplace and a lifestyle. For some organizations, it is enabling new business models. For others, it offers a new way of engaging with customers. For many more, it represents an entirely different way of doing business and working with ecosystem partners. Organizations are building digital strategies and deploying and provisioning digital technologies. One certainty in today’s environment is that most could not survive for very long today without their digital systems; indeed for some, technology provides the source of their competitive advantage while, more often than not, it is a necessity just to survive and avoid being disadvantaged.

As they embark on so-called digital transformation journeys, many companies are struggling to embrace digital opportunities and rewire themselves as digital organizations. While technology can be a constraint as well as an enabler of strategy and organizational agility, being digital is not a technology challenge but one of knowing how to get things done. Let’s assume that an organization moves all its IT infrastructure, applications and services “off premise” and into “the cloud.” It does not now follow that the requirement to build a digital strategy, seek innovative digital opportunities, design the organization’s architecture, prioritize and make digital investment decisions, or run projects and programs to implement digital strategies all suddenly disappear. As in the past, these requirements are all still paramount, together with the need to define a sourcing strategy, specify service expectations, assess, select and negotiate with vendors, achieve integration across multiple cloud providers and manage the delivery of myriad services. What all these functions have in common is that they are intellectual endeavors requiring the application of knowledge. Moreover, this knowledge is not located in any one organizational unit; rather, it is dispersed across the organization and requires coordination and integration to create “the knowing how to get things done” for these functions to manifest themselves. Having this knowing how is the objective of a digital capability.

In this chapter we introduce the scaffold for a digital capability. We first develop the arguments that embracing digital is a knowledge-based quest, and as this knowledge is distributed across an organization it presents a challenge for its coordination and application.
Furthermore, we argue that the essence of embracing digital is not to manage technology per se but to manage for the delivery of value from the capabilities of technology. Having presented its theoretical underpinnings, we first propose scaffolding upon which to hang the elements that make up a digital capability. We then explore how this “knowing how” is achieved. The chapter concludes with suggestions as to how organizations can begin the process of building a digital capability.

From managing technical artifacts to harnessing distributed knowledge

When computers first entered organizations, the expectation for them was limited to the automation of repetitive tasks through the processing of data. This objective was eloquently captured with the label attached to this quest: electronic data processing, or EDP for short. Primarily concerned with payroll and some accounting tasks, computers were seen as improving efficiency and cutting costs. Those organizations that could afford a computer established a separate unit (typically referred to as the computer or EDP department), staffed by technologists, whose job it was to keep this machine running. These professionals had the knowledge, skills and experience to maintain the hardware and software. As early computers were both physically large as well as being expensive to purchase, the majority of organizations availed of the services of computer bureaus, purchasing time share. This usually necessitated physically bringing punched cards and magnetic tape containing the data to be processed to the bureau; indeed, this can be considered as the forerunner to today’s outsourcing practices. However, and this is the key point, the role of technology was very much peripheral to the core activities of the organization.

But this all changed in the early 1970s. As technology advanced and computers became more affordable, there was increasing use by organizations of “on premise” technology, with many purchasing their own computers, building data centers and deploying packaged software. With the emergence of the personal computer (PC) and networking offering connectivity between devices, corporate computing was given a massive boost in the 1980s. As an inflection point, it also signaled a shift away from solely investing in technology for efficiency objectives to proactively seeking opportunities for competitive advantage. The role of technology had fundamentally changed, and this was accelerated with the opening up of the Internet for commercial activity in the early 1990s and, more recently, with the emergence of smartphones, cloud computing and the Internet of Things (IoT). Yet this shift is not generally reflected in how the majority of organizations choose to manage IT.

In much of the literature, the dominant practice is to objectify IS (in fact, “IS” and “IT” are generally used interchangeably), portraying it as data, information (sometimes knowledge), systems, hardware, software (including licenses), contracts, staff and associated costs (e.g., development, maintenance). As such, it is depicted as something – essentially artifacts – that can be directly manipulated. Even with outsourcing, the decision is typically framed as deciding what activities and resources should be sourced externally; the outcome of any decision to outsource is characterized as managing contracts, the supply of services (i.e., through service level agreements, service catalogues, and change requests), and relationships. It is likely that this logic sees organizations maintain an IS unit as a separate organizational entity, the assumption being that IS, as an objective construction, is manageable from within this structure. Importantly, what it suggests is that everything to be managed can be ring-fenced and contained within clear organizational boundaries. This unit can then be assigned a head (i.e., the CIO), given resources and a mandate that is often framed as optimizing or maximizing a return from any spend, all of course within an acceptable level of risk.
Moreover, the concept of “IT management” (IT eventually replacing the label “computer”) dates back to an era when computers were large, complex and expensive, requiring specialist facilities and knowledge, where the key challenge for IT professionals was to keep the computer functioning. The practice of IT management thus became associated with the activities to keep the machine working, with requirements evolving over time to encompass the design and implementation of systems and the provision and presentation of information. And while the concept of information systems (as opposed to IT) management is now in common use, the tasks ascribed to IS management have expanded to include IS/IT strategy formulation and execution, innovation, IT service management, IT implementation, project management, managing software development projects, protecting information assets, technology and service procurement, vendor management and, in many cases, the delivery of expected benefits from IT investments.

In fact, the notion of IS (or IT) management is tautological, equating to the management of IS (or IT)! It conjures up the notion that ontologically, information systems are something that can actually be managed. Perhaps this is why leadership teams that are disappointed with the perceived return from their IT investments instigate programs to improve the performance of their IS organization; the assumption being that this is where the genesis of this problem lies (after all, this is the organizational unit responsible for IS (or IT)). Indeed, studies reporting on such initiatives typically begin with this proposition (Peppard, forthcoming). For example, Cross et al.’s (1997) presentation of the transformation of the IS organization at British Petroleum noted that “the IT function of the exploration and production division of British Petroleum Company set out to transform itself in response to a severe economic environment and poor internal perceptions of IT performance” – the ultimate sanction being to outsource the function, or parts of it, to a third party.

If we take a contrasting perspective, where the managerial challenge is not to manage IS (or IT) per se, but to generate value from IS – note that we are not specifying what this value is other than have a positive impact on organizational performance – then a somewhat different agenda emerges. This viewpoint accommodates IS in organizations as a situated and socially constructed phenomenon, questioning the very nature of what is sought to be managed. Specifically, it proposes that IS is not a “thing” or set of “things” that can be managed or manipulated directly but that generating value from IS is a multifaceted and complex challenge. It necessitates understanding how technology impacts industry and competitive dynamics, identifying strategic opportunities, assessing and assimilating technological innovations, deriving new technology-enabled business models and organizational blueprints, prioritizing investment opportunities, managing IT-enabled change, deploying appropriate technology, steering IT projects, managing risk, selecting and managing vendors, exploiting investments in technology, ensuring appropriate usage of information systems, creating the environment for staff to embrace the right behaviors and values to work with information, and ensuring that the value delivered from any application of IT is captured by the organization. All related activities, practices and processes cannot happen within the confines of a separate organizational unit, labeled the IS organization, but are pervasive organization-wide concerns and endeavors.

Moreover, all these activities and related practices are underpinned by the application of knowledge, knowledge that is distributed across the organization. Software applications themselves are the automation of organizational knowledge that is made explicit and embedded in workflows that capture algorithmic logic. In fact, technical infrastructures are the embodiment of knowledge, knowledge that has been deployed by systems and solutions architects, software developers, networking experts and so forth in its design and construction. Maintaining
this legacy also requires knowledge, and while much of this knowledge will be primarily technical, some knowledge of business imperatives will also be required – for example, making the decision as to whether to decommission an application will depend on whether it is required by the business. Outsourcing arrangements can be similarly viewed as having a basis in knowledge (Kotlarsky et al., 2007); indeed, many organizations argue that they have outsourced their IT to an external service provider (ESP) or vendor, as it will provide them with access to knowledge that they do not currently possess. The challenge in generating value from IS can therefore be framed as one concerned with coordinating and integrating this knowledge to create organizational knowing, knowing how to get things done.

Yet, managing IT (or IT management) has never really been about technology anyway. It has always been a knowledge-oriented undertaking. Even in the 1960s and '70s, keeping complex mainframe computer systems functioning required specialized knowledge, most of it of a technical nature. And, when this was the only requirement, this knowledge was probably best housed within a separate organizational unit. Importantly, it was all under the jurisdiction and control of a single individual with a clear responsibility. Keeping technology functioning is not analogous to the delivery of value from technology; this challenge is much broader in scope.

The perspective of knowledge subscribed to in the foregoing discourse is that it is a social construct and “embodied” (Blackler, 1995) rather than an objectively definable commodity. As such, it is disseminated and legitimated within organizations through an ongoing process of interaction among individuals. Communication therefore plays a key role, with language itself similarly embodied in character. It is through these interactions taking place at multiple levels and among multiple employees that this knowing is developed. Organizational knowing can be seen as “an ongoing social accomplishment, constituted and reconstituted as actors engage the world in practice” (Orlikowski, 2002, p. 249). This knowing is at the heart of the digital capability.

Thus, what is being claimed is that the necessary knowledge underpinning this knowing to deliver value from digital is distributed throughout the organization (Peppard, 2007). Crucially, it is not located solely in a separate IS unit and under the jurisdiction of the CIO. In fact, much of this knowledge is under the control of other C-level executives. This is why, for example, it has been stressed as being of crucial importance for the CIO to build relationships with these executives – to ease access to knowledge resources under their control. If not, access to this knowledge will be difficult, if not impossible. Even with access, the organization must have the capability to coordinate and integrate this knowledge (Grant, 1996). This requires not just having a personal network providing access to knowledge, but also demands that trust, shared understanding and cooperation exist between parties for collective action to happen. Moreover, interactions via conversations play a central role, but this requires the ability to represent the knowledge of others. The not unreasonable assumption is that if all necessary knowledge cannot be harnessed, organizational knowing will be weak and it will be unlikely that value from digital will be optimized.

Digital can be seen as an umbrella term for both IS and IT, having both technological and information and system components (Peppard and Ward, 2016). A digital capability can be characterized as an organization’s ability to continually generate value from information, systems and technology (Peppard and Ward, 2004). All organizations require a digital capability even if an organization makes the strategic choice not to seek competitive advantage by being an early adopter of new technology. As technology, via its information handling capabilities, permeates all activities and areas of an organization, having a digital capability becomes a necessity. Building a digital capability is not about constructing a technological infrastructure; rather it is a challenge about creating organizational knowing.
The theoretical underpinnings of a digital capability

To provide a theoretical underpinning for the digital capability we draw on the resource-based view (RBV) of the firm that has emerged from the strategic management discipline. This theory points to the importance of internal firm-specific factors in explaining variations in the performance of organizations, particularly over a period of time (Barney, 1986a, 1986b, 1991, 2001; Cool and Schendel, 1988; Hansen and Wernerfelt, 1989; Rumelt, 1991; Wernerfelt, 1984). A basic assumption of the RBV is that resources (i.e., technology, knowledge, skills) are distributed heterogeneously across organizations (Barney, 1991). The theory argues that it is processes of resource accumulation and deployment that lead to idiosyncratic endowments of proprietary “assets” (Collis and Montgomery, 1995; Dierickx and Cool, 1989; Peteraf, 1993; Prahalad and Hamel, 1990; Wernerfelt, 1984) which may contribute to sustainable competitive advantage (Teece et al., 1997). These assets are typically referred to as competences. While RBV is ostensibly a theory of competitive advantage, it can also be useful when exploring firms at an individual level and how they harness resources to get things done.

Central to the RBV perspective is the fact that resources, per se, do not create value (Bowman and Ambrosini, 2000; Penrose, 1959); value is created by an organization’s ability (or competence) to utilize and mobilize those resources. In the context of generating value from digital, as a cognitive challenge, the critical resource is the knowledge residing in employees or the employees of third-party vendors. Competence represents an organization’s ability to deploy combinations of specific resources to accomplish a given task (Amit and Schoemaker, 1993) and is therefore the ongoing knowing that is enacted through the everyday and ongoing work of employees (Orlikowski, 2002). Thus competences are the collective knowing of the organization in initiating or responding to change “that is built into the organization’s processes, procedures and systems, and that is embedded in modes of behavior, informal networks and personal relationships” (Collis, 1996, pp. 149–150).

An organizational capability is the strategic application of organizational competences (Kangas, 1999; Moingeon et al., 1998). In the context of digital, the capability is determined by the existence and strength of the underpinning competences. The hierarchy of capability, competences and resources that can be drawn from the RBV literature is illustrated in Figure 19.1.

A reasonable assumption is that these digital competences are generic across all organizations; that is, all organizations require certain know-how to do things and achieve particular outcomes. Of course, how they might choose to build and execute competences can differ. We also assume that the strength of these competences will be determined by the required capability.

A scaffold for the digital capability

Having introduced the theoretical background, this section builds scaffolding for positioning the digital competences that underpin a digital capability. The core pillars of this scaffold are
derived from the basic models of alignment positing a relationship between business strategy, the portfolio of technology investments and performance (e.g., Henderson and Venkatraman, 1993). However, most of these models are based on an assumption that in achieving alignment, any expected value (which is usually not defined) will be guaranteed, omitting that it is the actual usage of information in organizational and inter-organizational processes and by humans that ultimately delivers value (Devaraj and Kohli, 2003). Acknowledging this, the three core pillars of the accommodating scaffold for the digital capability are strategy, technology and use (see Figure 19.2).

It is the strategy pillar where the thinking takes place about how technological capabilities will be harnessed both in enabling and shaping corporate and business unit strategies; these capabilities are centered on technology’s ability to handle information (i.e., capture, process, manipulation, store, retrieve and present). However, any strategy merely sets out the intent – we know that the success rate of IT projects to implement strategic choices is not stellar. The strategy will also accommodate the organization’s appetite for risk that determines, to some extent, its willingness to embrace new and emerging technologies. The technology pillar focuses on the required capabilities of the enabling technologies. Use is concerned with utilizing information to positively affect the performance of processes, support decision making and generate insight.

The linkages between the three pillars are important and they are also illustrated in Figure 19.2. In summary, these linkages can be described as follows:

- **Exploration/exploitation**: Information can be leveraged through either its exploration or its exploitation and the strategic intent determines the nature and extent of this. Organizations have traditionally used technology in an exploitative mode, where information is objectified and manipulated and is the essence of using technology to affect the performance of organizational process. Exploration is where data is interrogated to uncover insight, with technologies capabilities augmenting human cognitive processes.

- **Deployment/provisioning**: While technology provides information handling capabilities, this technology can be built and managed in-house, provisioned from external sources, or most likely today, be a combination of both “on premise” and external resources and services.

![Figure 19.2](image-url) Basic scaffolding for a digital capability
Changes/services: It is through programs and projects – devices for implementing the strategic intent – that changes in the organization are shaped and enabled. If managed well, these should lead to the achievement of expected outcomes. These changes in both processes and information use by employees are then sustained by the resultant services delivered by the capabilities of technology.

The objectives of these three linkages are well established and these domains are illustrated in Figure 19.3. The nature and extent of exploration and exploitation is determined by the IS strategy. The IT strategy provides the strategic framework for the supply of technology. The use of information is predicated by, among other issues, the quality of the information system and also how well the data handling capabilities provided by technology are delivered.

The IS strategy essentially articulates how the organization plans to both explore and exploit information. It is concerned with defining the operating model, including both process logic and information flows, determining the extent of information integration and process standardization and the applications (of technology) that will be required to execute the strategy. The IT strategy provides the overall strategic framework for the supply of technology capability. It frames the extent of insourcing and outsourcing. It also addresses issues of security and the protection of information assets. The final domain emphasizes IS and IT strategy implementation and ongoing sustainment of the organization. It defines how programs and projects to implement the strategic intent will be set up and run as well as how the delivery of resultant services, which will sustain these changes (and the realization of the organizational design), will be managed. Best practice program and project management methodologies and processes are often adopted here to deliver in change, such as a new customer management process. Industry standard best practice processes, such as ITIL, are used to assure the quality of IT services.

Digital competences

The three pillars and core domains represent the areas of competence underpinning the digital capability. These six areas are referred to as macro-competences. Using a multi-method
research approach, previous research (Peppard et al., 2000) identified 26 micro-competences distributed around these macro-competences. Over the intervening period, these competences have been refined and the most recent research distinguishes 31 such micro-competences that can be positioned around the scaffolding of the digital capability. These are presented in Table 19.1.

Table 19.1 Macro- and micro-competences definitions

<table>
<thead>
<tr>
<th>Macro-competence</th>
<th>Micro-competence</th>
<th>Knowing how to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crafting strategy</strong></td>
<td>Identify and evaluate the implications of IT-based opportunities as an integral part of business strategy formulation and define the role of digital</td>
<td></td>
</tr>
<tr>
<td>Business strategy</td>
<td>. . . ensure that business strategy process identifies the most advantageous uses of information, systems and technology</td>
<td></td>
</tr>
<tr>
<td>Digital innovation</td>
<td>. . . incorporate the potential of new and emerging technologies in long-term business development</td>
<td></td>
</tr>
<tr>
<td>Investment criteria</td>
<td>. . . establish appropriate criteria for making decisions on digital investments</td>
<td></td>
</tr>
<tr>
<td>Portfolio management</td>
<td>. . . optimize the overall value from IS/IT spend ensuring that the portfolio of investments in digital produce the maximum return from resources available within risk parameters</td>
<td></td>
</tr>
<tr>
<td><strong>Defining the IS requirement</strong></td>
<td>Translate the business strategy into information, systems and process investments and change plans that match the business priorities (i.e., the IS strategy)</td>
<td></td>
</tr>
<tr>
<td>IS strategy alignment</td>
<td>. . . ensure that IS development plans are integrated with organizational and functional strategic plans</td>
<td></td>
</tr>
<tr>
<td>Information quality architecture</td>
<td>. . . specify data/information quality criteria architecture specifying extent of process standardization and information integration</td>
<td></td>
</tr>
<tr>
<td>Organization information infrastructure</td>
<td>. . . determine the overall process and information infrastructure to achieve strategic and operational objectives</td>
<td></td>
</tr>
<tr>
<td>Business process management</td>
<td>. . . identify, design, document, monitor and optimize the execution of an organization’s processes</td>
<td></td>
</tr>
<tr>
<td>Business improvement</td>
<td>. . . continually identify opportunities to improve process performance and information availability</td>
<td></td>
</tr>
<tr>
<td><strong>Defining the IT capability</strong></td>
<td>Translate the business strategy into long-term information architectures, technology infrastructure and resourcing plans that enable the implementation of the strategy (i.e., the IT strategy)</td>
<td></td>
</tr>
<tr>
<td>Infrastructure design and development</td>
<td>. . . define and design information, application and technology architectures and organization structures and processes to manage resources</td>
<td></td>
</tr>
<tr>
<td>Capacity forecasting and planning</td>
<td>. . . model and forecast the capacity required by the organization to meet demands for IT services, infrastructure, facilities and people</td>
<td></td>
</tr>
<tr>
<td>Technology analysis</td>
<td>. . . establish criteria and processes to evaluate supply options and contracts with suppliers</td>
<td></td>
</tr>
<tr>
<td>Sourcing strategies</td>
<td>. . . establish criteria and processes to evaluate supply options and contracts with suppliers</td>
<td></td>
</tr>
</tbody>
</table>

(Continued)
Macro-competence | Micro-competence | Knowing how to...  
--- | --- | ---  
**Using information**  
Service requirements | ... define service arrangements and performance criteria (service levels) to match the business requirements  
Risk | ... establish acceptable criteria for IT-related risks  
Realize the benefits intended from the implementation of digital investments through effective use of information, applications and IT services  
Informed decisions | ... make fact-based decisions in a given situation  
Generate insights | ... uncover new knowledge and understanding from information  
Benefits delivery | ... monitor, measure and evaluate the benefits derived from IS investment and use  
**Delivering change and services**  
Deploy resources to develop, implement and operate digital business solutions, which exploit the capabilities of technology  
Benefits planning | ... explicitly identify expected benefits from digital investments and plan to realize them  
Managing change | ... make the business and organizational changes required to maximize planned benefits without detrimental impact on stakeholders  
Applications development | ... implement, at an appropriate speed, information, systems and technology  
Service management | ... deliver, operate and control IT services offered to users meeting service-level criteria  
Information asset management | ... establish and operate processes that ensure data and information meet quality criteria  
Business continuity and security | ... provide effective recovery, contingency and security processes to prevent risk of business failure  
**Supply of technology**  
Create and maintain an appropriate and adaptable information technology and applications supply chain and resource capacity  
Supplier relationships | ... manage contracts and develop value added relationships with suppliers  
Technology standards | ... develop and maintain appropriate standards, methods, controls and procedures for the use of IT and associated resources  
Technology/service acquisition | ... develop and apply procurement policies and procedures for the organizational acquisition of infrastructure components and specialist technologies/services  
Asset and cost management | ... ensure technology, information and application assets are effectively maintained and costs of acquisition and ownership are understood and managed  
IS/IT staff development | ... recruit, train and deploy appropriate staff and ensure technical, business and personal skills meet the needs of the organization  
Technology infrastructure management | ... manage technical IT infrastructure during all life cycle phases, comprising all transitional activities (build, deploy, and decommission) and operational activities (operate/maintain and continuously improve)
This table describes the six macro-competences as well as defining each of the 31 micro-competences. The macro-competences have been labeled slightly different from Figure 19.3 to make them more evocative of what is being sought. The micro-competences are, in effect, the 31 “knowing how to . . .” competences that capture the organizational knowing that underpins the digital capability.

**Leadership and governance**

Over the decades, research has stressed the importance of leadership and governance in the success of digital. However, both are often mistakenly seen as competences that organizations should develop. It is our contention that neither is an organizational competence, rather they frame the digital capability (see Figure 19.4). Without the right leadership and support, organizations will struggle to embrace digital opportunities and deliver any expected business outcomes. This leadership must come from not just the CIO but also the whole leadership team (Weill and Ross, 2009). Digital may have technology connotations but is a critical business issue.

Establishing an appropriate governance structure for digital is also vital (Sambamurthy and Zmud, 1999; Schwarz and Hirschheim, 2003; Weill and Ross, 2004; Zmud, 1984). This is because many decisions, previously considered as falling to the IT professional to make (when all knowledge could be corralled into a specific organizational unit), require active business involvement, sometimes even accountability. Consequently, mechanisms are required to ensure coherence in all decisions made in respect of digital, particularly when decision making is both devolved and distributed (Weill, 2004; Weill and Ross, 2004; 2009).

![Figure 19.4 Leadership and governance: framing the digital capability](image-url)
The governance structure should support the behaviors that are deemed necessary in respect of digital and specify clear accountabilities. Governance mechanisms, such as IT steering committees and other cross-function forums, are established to coordinate the consequence of devolvement as well as encourage the involvement of relevant parties in decision-making processes. These forums are operating outside of formal structures – within the so-called informal organization – and are central to creating an environment for knowledge access and integration (Chan, 2002; Preston and Karahanna, 2009; Tan and Gallupe, 2006). While governance structures mandate that decisions traditionally made within the IT unit be devolved out of the remit of the CIO and IT unit altogether and into the realm of business executives, there can be both reluctance and resistance from business executives to assume these new responsibilities. This points to the importance of not just knowledge but also behaviors and values – an issue that we shall address in the next section.

Establishing an IT governance structure is giving tacit recognition that what are often labeled “IT decisions” are essentially decisions that require the coordination and integration of knowledge that can be dispersed across an organization. Even expertise in technologies is also migrating away from IT professionals and becoming more embedded in those with functional responsibility; for example, social media in the marketing organization and analytics and business intelligence (BI) in finance departments. Many applications can now be delivered directly from “the cloud,” with end users potentially bypassing corporate infrastructures and, more crucially, the IS organization itself leading to the presence of “shadow IT.” With the Internet of Things, there is increasing danger of applications being built outside of an organization’s architecture.

**Building digital competences**

Building the digital competences is an organization-wide endeavor. As emphasized throughout this chapter, the challenge is to bring together those with the relevant knowledge to create the necessary knowing. This is easier said than done. It is worth acknowledging that historically many CIOs have attempted to facilitate access, coordination and integration of knowledge, although they may not always recognize this as the objective of the initiatives they promoted. For example, many have appointed relationship managers as a conduit, facilitating knowledge exchange between the IT unit and different parts of the organization. While such initiatives seek to provide access to knowledge they may, however, not directly impact its integration. In reality, relationship managers typically act as translators of requirements or reporters of problems. Establishing governance structures, such as committees and other cross-organizational forums, bring individuals with relevant knowledge together to debate particular issues related to IT, make specific decisions and have oversight on decisions and outcomes. Yet, even where people come together in such forums, they may choose not to share their knowledge.

Some CIOs have established educational programs to improve IT staffs’ knowledge of the business, creating so-called hybrid managers (Skyrme, 1992). This overcomes the fact that it can be difficult to get business engagement, that is, access to their knowledge, with the CIO attempting to build this knowledge inside the IT unit. However, this does not defeat the requirement for business and IT people to cooperate and work together, that is, to integrate and coordinate their knowledge. To this end, education programs for non-IT staff are often instigated to create awareness of digital issues, build digital literacy and highlight their role in delivery of the expected benefits of digital investments. The assumption is that this understanding communication will be forthcoming; usually this requires some priming.

Initiatives like chargeback, where users are “charged” based on the IT resources and services they consume, can serve to foster communications between IT and the business units (Ross et al., 1999). Such communication can generate a rich shared understanding for both
parties of the cost and benefits of alternative IT investments and service offerings. Indeed, research shows that a high level of communication between IT and business executives is a direct predictor of alignment of business and IT strategies (Reich and Benbasat, 2000).

Thus, while knowledge is “owned” by the individual, the integration of this knowledge to create knowing and understanding takes place at a collective level: groups and other collective forums, some of which are formal and others informal (Okhuysen and Eisenhardt, 2002). Although specialist knowledge is required to accomplish many tasks in an organization, there are also situations in which individuals with specialized knowledge must represent and integrate their knowledge in a group or other collective to create organizational knowing. As we have seen, this is at the core of a digital capability.

To explore how that might occur, the notion of “social capital” offers an explanation of how distributed knowledge can be harnessed to create organizational knowing. With its origins in sociology, social capital highlights the importance of networks of strong, personal relationships, developed over time, across groups, units and geographies that provide the basis for trust, cooperation and collective action (Alder and Kwon, 2002; Nahapiet and Ghoshal, 1998; Tsai and Ghoshal, 1998). It also emphasizes behaviors. The theory suggests “that actors are motivated by instrumental or expressive needs to engage other actors in order to access other actors’ resources for the purpose of gaining better outcomes” (Lin, 2001). In the context of the digital capability, these “resources” are knowledge, and “better outcomes” is the organization knowing contributing to the competences.

Access to knowledge is dependent on an individual’s network of contacts and ties as well as the nature and content of the relationship between parties. Recognition of the value of collaboration is based on the ties that people have together with a shared language and cognition to aid mutual understanding. The motivation to share and combine knowledge and collaborate is underpinned by trust and obligations that can be defined by the role and position that individuals have in the organization. Figure 19.5 presents a schematic of this, illustrating that it is through people coming together that knowledge is shared and competences manifest themselves.

Figure 19.5  Social capital providing the environment for organizational knowing
Figure 19.6 attempts to bring together the earlier discourse about digital competences that draws on the RBV with the preceding discussion on social capital. It illustrates that at the resource level, knowledge resides in people, and that it is through people coming together in social contexts that organizational knowing emerges. Social capital theory can help understand the ingredients that need to be present for this to occur.

In a global reinsurance brokerage where we undertook research, the consequence of a strong digital capability was clearly evident. The company has recognized the value of information and its effective management for its competitive success. The CIO is a member of the board of directors and has a very strong partnership with the CEO. They regularly attend digital conferences together. The CIO is a key player in the business strategy process; one colleague noted, “I think that he is forward-thinking enough to be looking at new technologies and that he is brave enough to take the decision to go with things,” and this often means driving the business strategy. A quote from the company’s digital strategy document best illustrates how digital is deployed in the company:

Information systems cannot afford to wait for a clear and detailed specification of “strategy” from the business and customers it is trying to serve. It is more a question of applying IS/IT foresight to the situation, in order to make reasoned assumptions to an appropriate course of action.

There is also a close partnership between the IS unit (and staff in this unit) and the rest of the business. Indeed, this is probably helped, as the CIO is responsible for both IT and the bulk of business operations (the exceptions being marketing and risk management). Roles are clearly specified, particularly in the setup and management of projects and in the delivery of IT services. The philosophy of the IS function was described by one IT manager as “we help you to help yourself,” in reference to the fact that they work closely with the business. The company has not set out to develop and nurture the 31 digital competencies explicitly, but they are present. They do provide an explanation of why the company has probably been the most successful player in its industry over the last 20 years and recognized by its peers as being innovative regarding the harnessing of digital.
Conclusions

Nearly 30 years ago Dearden (1987) predicted the demise of the IT unit in organizations. The basic premise of his arguments were that “users” would soon completely control individual systems and that systems development would be done almost entirely by outside software specialists. However, it is unlikely that he foresaw the tremendous advances in technology and the key role it would play in business and global commerce. Yet while he was right that the IS organization, in its guise at that time, would wither away, he erred by suggesting its demise based largely on arguments focused on technology deployment. Focusing on value generation from IT presents a different conclusion. Rather than withering away, it has become pervasive.

This chapter argues that executives should no longer see the knowledge and the organizational knowing how that required to respond to digital challenges and opportunities as residing in a separate organizational unit under the control of a single individual. Rather, this knowledge is distributed not only across the organization but can also be found in vendors and other third parties, perhaps even customers. The challenge is to coordinate and integrate this knowledge to build the necessary organizational knowing. In this chapter we have suggested that it is achieved by building 31 competences and that these underpin a digital capability. The perspective presented in this chapter emphasizes the essential role of human action in knowing how to get things done that lies at the heart of a digital capability.

While the existence of a strong digital capability may be observable (if not yet measurable), we still do not know precisely the individual knowledge components (perhaps better referred to the “know-what”) of each underpinning competence (the knowing or “know-how”); more research is needed to determine this. Moreover, it is likely that uncovering actual practices will illuminate further the knowing that is enacted through the everyday and ongoing work of employees. Uncovering these practices will demand immersion in study sites.

Notes
1 The colloquial term for cloud computing.
2 Originally they were referred to as servers.
3 Any discourse around this question raises the wider issue as to what IS (both singular and plural) actually is/are and is beyond the scope of this chapter. Interesting insights can be found in Alter (2008), Beynon-Davis (2010); Bryant (2008), Paul (2010) and Lee et al. (2015). For an exposition of the relationship between IS and technology, see some of the recent research on socio-materiality (Orlikowski, 2010; Scott and Orlikowski, 2013; Orlikowski and Scott, 2008; Orlikowski and Iacono, 2001). For extended treatises on what constitutes the IS discipline, see Banville and Landry (1989), Benbasat and Zmud (2003), Somers (2010) and March and Niederman (2012).
4 The view of knowledge that accommodates this is that it can be objectified and made explicit, therefore making it possible “to code” the logic into software programs.
5 It is not our intention to engage in a debate as to whether it is actually a “view” rather than a “theory.”
6 The literature is confusing in its usage of the labels “competences” and “capabilities.”
7 The RBV has been used by scholars to explore the contribution of IS resources and capabilities to performance and competitive advantage. See, for example, Bhattacharyya and Grover (2005), Bharadwaj (2000), Doherty and Terry (2009) and Wade and Hulland (2004). For seminal research highlighting the role of internal resources in achieving competitive advantage from IS/IT, see Clemons and Row (1991) and Kettenring et al. (1994).
8 To reduce confusion, the use of the label “capabilities” in this instance refers specifically to the information-handling capabilities of technology.
9 ITIL is the IT Infrastructure Library and part of the services provided by the UK’s Office for Government Commerce (OGC). See A Code of Practice for IS Service Management, British Standards Institute, London, 1999.
References


Paul, R. J. (2010) ‘What an information system is, and why it is important to know this,’ Journal of Computing and Information Technology, 18(2), 95–99.


