June 2012

Leveraging cyber safety opportunities to build sustainable competitive advantage in a Victorian private school

Kim Stock[1]

Abstract

A Victorian private school, *XYZ,* has launched an innovative cyber safety initiative to support parents and students in navigating complex situations in the digital world. The aim of this research is to develop a SWOT analysis of the *XYZ* initiative to identify sources of potential competitive advantage, and leverage the human and technical resources underpinning those sustainable competitive advantages. This report is important because there is little research exploring the identification of sustainable competitive advantage using SWOT analysis in the private school sector, and this research will provide an opportunity for *XYZ* to develop effective strategic actions to maximise the impact of their cyber safety initiative. The research methodology was interviews with *XYZ* management, functional and academic staff, and clients. A literature review of current cyber safety research in the US and Australia and the cyber safety practices on the websites of relevant competitor schools provided contextual data. A Dynamic Capabilities Framework was developed to provide characteristics to identify potential sources of sustainable competitive advantage from the SWOT analysis. The research found that *XYZ* was a market leader in the provision of a cyber safety website; however, this was not a sustainable competitive advantage. To maintain sustainable competitive advantage the strategic focus of *XYZ* requires a shift toward excellence in the quality of the behavioural aspects and academic integration of the cyber safety support service.

Keywords: cyber safety, competitive advantage, private school, SWOT analysis, dynamic capabilities

[1]Human Resource Consultant at IVECO Trucks Australia Pty Ltd

Leveraging cyber safety opportunities to build sustainable competitive advantage in a Victorian private school
Kim Stock

Introduction

Traditional sources of competitive advantage, such as economies of scale and huge advertising budgets, are no longer enough in the twenty-first century global economy; instead, managers must adopt new strategies that use flexibility, speed, innovation and integration to exploit the challenges that evolve from constantly changing conditions (Hanson, Hitt, Ireland & Hoskisson 2011). Crafting and executing effective strategies can create value for an organisation by providing a road map to navigate these challenges. Most high achieving organisations rely on creative, proactive strategy making to set their organisation apart from their rivals (Thompson, Strickland & Gamble 2008).Strategy making involves a strengths, weaknesses, opportunities and threats (SWOT) analysis to combine the evaluation of the organisation's external opportunities and threats with an analysis of the organisation's internal resource strengths and weaknesses. SWOT provides a simple comprehensive method to combine an external and internal perspective when crafting strategy.

In Australia, little research has explored the identification of sustainable competitive advantage using SWOT analysis in the private school sector. Previous Australian case studies using SWOT analysis to identify sources of competitive advantage were based on traditional manufacturing, retail and the scientific research and development industries (Rice, Martin, Carpenter & Sanders 2010). This identification of sustainable competitive advantage is an important requirement of strategic analysis and fundamental to an organisation's long term success (Thompson et al. 2008).

The aim of this research is to undertake a SWOT analysis of a private school's cyber safety strategy initiative and identify sources of sustainable competitive advantage. The case study findings will benefit managers in the private school and education sectors and other industries identifying sources of competitive advantage applicable to their own organisations in dynamic environments.

The following section provides background about strategic management in general and this case study in particular. Section 3 describes the research methodology and findings from the cyber bullying literature and interviews; the data analysis includes a SWOT analysis and a dynamic capabilities analysis. The final section includes key lessons and recommended actions.

Orientation

Strategic management. Organisational success can be defined as attaining a competitive position that leads to a superior and sustainable financial position (Porter 1985). Porter's (1985) five forces model of competition provides a framework for evaluating industry structure by analysing the degree of rivalry, the threat of new entrants, supplier power, buyer power and the threat of substitutes in the chosen industry. The five forces model evaluates industry attractiveness; however, success in an industry is based on two areas: industry attractiveness and the organisation's relative position in that industry. An attractive relative position is defined as possession of a sustainable competitive advantage over rivals, where competitive advantage results from the organisation's ability to perform the required activities at lower cost or in unique ways that create value. These activities include human resources, purchased inputs, and processes (sometimes called business routines) and each of those activities also use and create information (Dyson & O'Brien 1998). Performance of activities, individually or linked as a group, not only creates tangible assets but also creates intangible assets, including skills, capabilities, organisational routines and knowledge, which can appreciate over time. Intangible assets can be external to the organisation such as brand image, reputation, relationships and networks.

A SWOT analysis captures both these internal and external perspectives by evaluating the organisation's internal and external assets, strengths and weaknesses, and the organisation's relative position in the industry, opportunities and threats. Organisations interpret the SWOT list to understand their overall situation and determine strategic actions to better align the

organisation's strategy to its resource strengths and market opportunities, as well as guard against weaknesses and external threats in a bid to gain sustainable competitive advantage (Thompson et al. 2008).

There are two reasons why organisations gain competitive advantage over rivals: initial conditions, where organisations have pre-existing reputations, skills and routines as a result of their history; and through managerial choices, where management choices are made under conditions of uncertainty that lead to the creation and coordination of particular skills and resources (intangible assets) required to carry out the new strategy (Porter cited in Dyson & O'Brien 1998). The origins of competitive advantage are the bundle of valuable resources (or core competences) that the organisation possesses which are often intangible assets such as skills, reputation and business processes.

But these bundles of resources are not static. The dynamic capabilities approach to competitive advantage addresses the ability of organisations to modify, reconfigure, and upgrade resources and capabilities to respond strategically to, or generate changes in, the environment (Rice et al. 2010). That is, where an organisation can go depends on its history (current position) as well as the paths ahead (path dependencies), and so a SWOT analysis approach becomes a matter of leveraging internal strengths and weaknesses against developing external opportunities and threats. 'Dynamic capabilities thus reflect an organization's ability to achieve new and innovative forms of competitive advantage given path dependencies and market positions'(Leonard-Barton 1992 cited in Teece 2008, p.34; Porter 1985).Based on this insight, a dynamic capabilities framework has been developed as a diagnostic checklist to determine the dynamic capabilities from an organisation's SWOT analysis data (Teece 2008).

These strategic management ideas had not been employed in the *XYZ*private school's cyber bullying strategies.. The school provided unique access to a case situation to use these strategic management ideas about SWOT and dynamic capabilities.

The case organisation's background. The focus case organisation*XYZ* is a private co-educational school with enrolments of approximately 1800 students across three campuses. *XYZ* currently runs a compulsory laptop program for all students from year 5 to year 12. As a result of a strategic review in 2009/10, *XYZ* adopted a differentiation strategy in its approachto the private school market emphasising the value added, 'The *XYZ* Factor', to be its unique market proposition. This branding approach relies on the customer valuing the unique product and the existing reputation of the school. The strategy, which launched in early 2011, concentrates on five key areas: 1) 'state of the art' student learning; 2) enhanced curriculum; 3) school and family values; 4) human resource structure and development; and 5) enhanced physical facilities.

Whilst conducting the strategic review, the need to respond to changes in the cyber environment was highlighted. In response to recent emphasis by the media and government authorities in Australia and the United States described in the next section, many Australian schools have been reviewing and upgrading their cyber policies to deal with the new and rapidly changing cyber environment (The Alannah and Madeline Foundation 2010; Gillard 2010). Both educators and parents have voiced concerns about dealing with the new complexities of cyber bullying, cyber ethics and cyber security (National Cyber Security Alliance 2009).

As a result, *XYZ* formed a working party in May 2010 to look at ways the school could support its parents in dealing with internet-generated issues confronting their children, and a draft cyber safety policy and website were developed. In November 2010 the cyber safety website was launched at an invitation only event and an email was sent to all *XYZ* parents inviting them to view the website. In December 2010 the Principal of *XYZ* appeared on a national morning news program explaining the availability and benefits of the website to all parents around Australia.

Research question. Using recent research and *XYZ's* development of a cyber safety website and policy, the research study set out to identify some dynamic capabilities from the strategic management literature to leverage resources to gain sustainable competitive advantage.

Research methodology and findings

Case study research methodology is used to collect information relevant to specific research questions (Saunders, Lewis &Thornhill 2009). A single case can be justified because of its unique access to rigorous research (Yin 2008). Therefore a single case study using a combination of a literature review and an interview approach to collect primary data was appropriate to resolve the specific and practical question of how to leverage the introduction of *XYZ's* cyber safety initiative into sustainable competitive advantage. Moreover, the case study method is justified because the research is about promoting organisation change and involves a specific context, clear purpose, fact finding and analysis and recommended actions (Saunders et al. 2009). The research methodology was designed to incorporate each of these phases within four stages:

> Stage 1: Literature review of cyber safety environment
>
> Stage 2: Interviews of *XYZ* employees, students and parents
>
> Stage 3: Competitive data collection from public sources
>
> Stage 4: Analysis of data and development of SWOT.

Stage 1: Initial literature review of cyber safety issues

Stage 1 involved secondary research from Australia and overseas. The National Cyber Security Alliance (NCSA) (2008; 2010) sponsored studies exploring the nature of cyber ethics, cyber safety and cyber security policies, initiatives, curriculum and practices currently taking place in US education settings. A 2008 conclusion was that the curriculum content was limited, teachers did not feel comfortable with the cyber topics, issues were only addressed at a peripheral level and impediments to improvement were financial constraints,

time commitments, bureaucratic processes, and an already over packed curriculum (NCSA 2008). The 2010 report revealed that the most common cyber issues confronting teachers was 'cyber bullying' followed by 'sexting' (NCSA 2010). Cyber bullying is commonly defined as the use of information and communication technologies to support repeated and deliberate hostile behaviour intended to harm others, and sexting refers to young people using mobile phones to share images of themselves or others naked or participating in sexual acts (Australian Communications and Media Authority 2011). The 2010 study reflected the lack of a cohesive effort to provide students with the education they need to safely navigate the digital age and a failure to prepare them to be responsible digital citizens and employees (Kaiser 2010). Furthermore, the study reported that a high reliance on shielding students, instead of teaching behaviours for safe and secure internet use, was not preparing students to act more safely and responsibly when accessing the internet at home or through mobile devices (Kaiser 2010).

The 'Inquiry into bullying of children and young people' report prepared by a cyber safety expert for the Rudd Government in April 2009 identified that, although little academic research existed in Australia, the community had experienced similar cyber issues to the United States in educating young people about cyber bullying and that Australia also needed to develop educational programs to address the needs of young people, schools, parents and the wider community (McLean 2009).

In addition, a 2009 review of the current academic literature on young people and technology, conducted by Professor Helen McGrath, from the School of Education at RMIT University, found that in the new cyber age the relationship of teacher and student did not finish at the school gate and a duty of care may arise beyond it (Ford 2007, cited in McGrath 2009). That review concluded that there are important differences in the nature and handling of offline bullying and cyber bullying. Another university study in 2008 of the pedagogical challenges of cyber safety also provided an overview of the issues in an Australian context and concluded that applying traditional face-to-face strategies to cyber bullying was

simplistic and flawed (Hanewald 2008). That study recommended that a well researched and designed instruction course should be incorporated in pre-service teacher education programs and professional development programs for teachers, school counsellors and school leaders, and that it should include codes of practice for appropriate behaviour for students, teachers and parents.

The Australian Covert Bullying Prevalence Study concluded that cyber bullying was more prevalent among students from non-government (private) schools than those from public schools (Djakovac 2009).The Family-School & Community Partnerships Bureau website provided an overview of government cyber safety initiatives currently in progress, and of the website service of the Australian Communications and Media Authority (ACMA) called 'www.cybersmart.gov.au' (Anonymous 2011). It also discussed the development of a Joint Select Committee on cyber safety and a national pilot program to increase cyber safety in schools, and the launch of a government initiative, sponsored by the Alannah and Madeline Foundation, to assist schools develop their own cyber safety websites.

In brief, the literature indicated that notwithstanding the complexity of cyber safety it is of vital importance. Although a number of organisations are developing recommendations it is clear a great deal more is required.

Stage 2: Interviews

The second stage of the data collection was semi-structured interviews that were conducted by the researcher during November and December 2010. All interview participants were briefed on the purpose of the study and signed an informed consent form. Anonymity of all participants was guaranteed by the researcher; no individual is quoted in this report and the identity of teachers, parents and students interviewed was not revealed to *XYZ*. Because some participants considered anonymity crucial, taping of interviews was inappropriate. All

interview notes were transcribed by the researcher immediately following interview sessions and a summary of each interview cohort was generated after the cohort's interviews.

A more quantitative approach with survey questionnaires was not suitable because a survey methodology would not have provided opportunities to explore the ideas generated by the participants in as 'real a manner as is possible'. Moreover, supported by Stage 1's literature, the qualitative approach provided a more comprehensive and in-depth understanding of cyber safety and its relevance to the focus organisation (Robson 2002, cited in Saunders, Lewis &Thornhill 2009).

The interviewees selected for this research were representative of the *XYZ* secondary school environment. The 18 interviewees are more than the standard of 15 for academic research (Mason 2010). The *XYZ* staff interviews were conducted with eleven staff: four of the cyber safety committee members, the head of the largest *XYZ* secondary campus, two information technology staff, two senior years staff and two middle years staff. In addition, eight interviews were conducted with parents and students: two parents, and one male and one female student from each of the middle and senior year's cohorts. No participants from the primary school campus or the smaller secondary campus were included in the research due to time constraints and the logistics of visiting a regional campus. This limitation may have contributed some bias in the data; however, this was not significant enough to impact the overall validity of the data because approximately 70% of students in year 5 to year 12 relevant to the study attend the largest *XYZ* secondary campus.

Analysis of the interview data provided several key findings, firstly, the development of the cyber safety initiative at *XYZ* was seen as an important and positive strategy for the school by all staff groups; however, there was a general lack of consistency about the objectives of the cyber safety initiative between the committee group, teachers and the IT department and this was reflected in the uncertainty about the objectives among the students and parents interviewed. For example, there was uncertainty across each of the interview groups about

the expected role of each of the key stakeholders in the school's cyber safety environment. All staff interview groups confirmed that formal documentation of objectives and indicators for project success or performance measures for the cyber safety initiative project had not been developed. When asked to define what the nature of *XYZ's* cyber safety relationship with stakeholders should be, the terms 'supportive', 'shared responsibility' and 'partnering' were used in all groups.

Secondly, the quality and level of cyber safety and general communication was rated poorly by teachers, students and parents because it failed to engage recipients, was inconsistent, lacked transparency and was not linked to the curriculum and values of *XYZ*. The parent and student groups strongly felt that the sole use of email notification did not qualify as effective or engaging communication for important initiatives.

In addition, all interview groups considered integration of the cyber safety initiative with *XYZ's* curriculum, strategy and values was critical to success; however, the student and parent group were unfamiliar with the 'precise school values' as they had not been specifically mentioned 'in a while'. The parent group was unfamiliar with the current school strategy. Both the parent and teacher groups considered parental and school values important criteria to be used as the basis of decision making by students about cyber safety issues and dilemmas. The currency, relevance and credibility of cyber safety information were considered critical success factors across all interview groups. All groups considered audio-visual case studies and peer discussion groups to be the most engaging means of communicating and transferring the learning.

The challenge of involving all stakeholders in timely knowledge sharing and ensuring the flow of information into and from the cyber safety initiative was considered a critical success factor by staff, parents and student groups. But the IT group considered keeping the cyber safety information up to date was within their domain. This silo approach was criticised in comments by parent, teacher and student groups who were unsure exactly what the

boundaries of IT responsibilities and services were. The teacher group was dissatisfied with the integration of IT initiatives with real academic needs as previously these had not always translated into meaningful improvement in the learning environment.

The teacher, parent, and student group, who had personal knowledge of *XYZ's* handling of sensitive cyber safety dilemmas or incidents, felt that the staff involved handled one individual incident 'well' and they were satisfied with the school's response. The striking similarity of the perspectives of the teacher, parent and student groups around critical success factors may be a reflection of their effective and successful joint participation in handling previous cyber safety issues at the school.

According to all groups, the two most important criteria for measuring the success of the cyber safety initiative were parent and student feedback on how well the initiative met their needs.

The next finding was a perception of a lack of competence in documenting standardised, transparent, and consistent policies, actions and consequences. This was highlighted by the teacher, parent and student groups and many participants felt this was a significant contributor to inconsistent behaviour and wide variations in parent and student expectations.

The final finding from the interviews was that all groups believed the priorities, issues and learning needs are different for middle year and senior year levels, therefore any strategy initiative should be specifically targeted to address each student level appropriately. Students in the senior years group were specifically interested in increasing leadership opportunities for senior students in providing mentoring and leadership to middle years students on cyber safety. Parent, student and teacher groups consider cyber bullying, sexting and digital reputation the three most significant issues impacting students.

The parent, student and teacher groups considered an understanding of the behavioural aspects of dealing with issues of cyber safety the most important skill for teachers to develop. Managing change in a dynamic environment was also considered important as well as creating a learning environment and having up to date cyber knowledge. All groups considered the professional development of teachers to be the responsibility of the academic area with support and information provided by IT to meet academic needs.

Stage 3: Competitive data collection from public sources

In Stage 3, a review of the websites of a selected group of private school competitors in Melbourne was undertaken to collect public data on their approach and policies regarding cyber safety. A primary data survey of those organisations would have been a more accurate method; however, because the project was scheduled during the 'end of school year' period impacting all schools and because of the proprietary nature of the data, it was unlikely the survey would have achieved a satisfactory response level. Nevertheless, the secondary data collected is considered a valid indicator of *XYZ's* relative position in the market place regarding its cyber safety initiative as potential clients' (parents and students) initial perceptions about the quality of services schools provide is based on the imperfect data in public areas of websites. Nine private school websites, including *XYZ,* and one academic selection state school website, were reviewed in detail.

Key findings of this website review are:

- *XYZ* was the only school providing a dedicated cyber safety website. Four schools within the review group displayed cyber bullying policy information.
- Most of the schools featured strong mission and values statements and reported on the importance of technology in delivering their curriculum. The *XYZ* website home pages did not feature mission or value statements; however, the primary campus and smaller secondary campus web pages did mention school values.

- The most common technology policy featured on the websites was "An acceptable use agreement for students". One school stated their commitment to the importance of technology was reflected in their use of an ICT Strategic Planning Committee whose task is to coordinate IT across the school and develop responses to opportunities likely to arise in the future.
- Two schools included lengthy bullying policies, including cyber bullying, on their websites.

Stage 4: Analysis of data and development of SWOT

Using the data collected in stages 1 to 3, a SWOT analysis was prepared to overview *XYZ's* cyber initiative and is shown in Table 1. Using a Dynamic Capabilities Framework Checklist (see Table 2) each of the opportunities and strengths was compared with each of the three categories of the framework, processes, positions and paths, to see if they exhibited the characteristics of a dynamic capability. Weaknesses were also compared with the checklist to determine which resource investments designed to correct weaknesses are most likely to support existing, or contribute to development of new, dynamic capabilities. Finally, threats were compared to the checklist to determine if they had an impact on existing or developing dynamic capabilities to ensure risk management strategies could be prioritised to remove or minimise critical threats to competitive advantage. Combining the SWOT analysis with the Dynamic Capabilities Framework assists organisations to focus scarce resources on potential sources of sustainable competitive advantage by prioritising strategic actions in areas exhibiting dynamic capability characteristics. Several sources of potential competitive advantage were identified in the dynamic capabilities categories of 'organisation processes' and 'position' (Teece 2008).

Key findings were as follows. Firstly, the competitive advantage of the cyber safety website is unlikely to continue. Competitors' ability to imitate and the introduction of the federal government's national website will quickly erode the scarcity advantage of the *XYZ* website. However the website has placed *XYZ* in a competitive 'position' to utilise the learning curve

to build on *XYZ* reputational assets, expand organisational boundaries through supplier and professional association relationships and exploit other emerging opportunities to expand *XYZ's* offerings to meet a broader range of client needs.

Secondly, deficiencies in *XYZ's*organisation processes were identified: integration, communication, knowledge management, project management and organisation structure and flexibility. They need to be addressed because the improved sources of tacit knowledge and business routines could contribute to 'difficult to imitate' dynamic capabilities and underpin *XYZ's* existing strengths. The most significant threat identified was potential damage to *XYZ's* reputational asset, a key source of its competitive advantage, if the website was marketed prior to establishing knowledge management procedures, creating key staff development documentation and comprehensively rolling out the initiative to *XYZ* staff and existing clients.

Table 1   **SWOT analysis of *XYZ's* cyber safety initiative**

Potential resource strengths and competitive capabilities	Potential resource weaknesses and competitive deficiencies
- Emerging strategy/opportunity identification - Strong brand name/reputation - Learning/experience curve in cyber environment *XYZ* cyber website is proprietary technology - Strong advertising and promotion - Relationships with suppliers of technology (e.g. Microsoft & ISV Project Victor, *XYZ* Project ICT) - Quality of selected teaching staff who successfully handle cyber issues in school environment - Laptop program and *XYZ*network	- Strategic alignment and link to values, vision and mission not well understood - Informal integration processes - Communication processes - Documentation of policies, materials, procedures, role definitions, expectations and consequences - Knowledge management processes (keeping up to date, in/out flow of information) - Lack of engagement and involvement: teachers, parents, students - Depth of behavioural skills across broader staff group (large variance in knowledge and skill level) - Poor internal marketing of technology innovation - Lack of formal project management processes/methodology - Functional reporting structure and administrative bureaucracy inhibits integration, flexibility and adaptability in dynamic environments - No link from objectives to success/performance measures
Potential market opportunities	**Potential external threats to *XYZ's* future prospects**
- First to market in cyber support - Rising buyer demand for cyber support services - Backward integration with IT suppliers (ICT strategic plan) - Exploiting new technologies - Expanding *XYZ* offerings to meet a broader range of customer needs - Exploit cyber leadership opportunities through private schools association and professional associations (IT, teachers)	- Erosion of advantage of website by competitors (imitation) or the launch of proposed national website by government ('eSmart') - Rapid changes in market may make website obsolete - Launching website before developing processes, maintenance procedures and engaging the *XYZ's* current staff and client groups exposes *XYZ* to avoidable risks which impact credibility/reputation including: - failure to maintain currency of website - disenfranchise existing parents

Table 2   **Dynamic Capabilities Framework Checklist**

Category	Characteristics indicating dynamic capabilities
Organisational & Managerial Processes	• **Coordination/Integration Processes** (static concept) - Static concept - Internal: activities inside the firm - External: sourcing and integration of external activities and technology • **Learning** ((Leonard-Berton 1995) cited Teece 2008) - Organisational as well as individual skills - Requires common codes of communication & coordinated search procedures - Knowledge generated by learning is captured in new patterns of activity, in routines or a new logic of organisation • **Reconfiguration & Transformation** - Ability to sense the need to reconfigure the firms asset structure is important in rapidly changing environments ((Langlois 1994) cited Teece 2010) - Requires constant surveillance of markets & technologies & the willingness to adopt best practice, benchmarking most useful - Change is costly, need to develop processes to minimize low-pay-off change initiatives - Decentralization & local autonomy support/denote 'high-flex' firms and support the process
Positions	• **Technological Assets** - Key differentiators among firms • **Complimentary Assets** - Technology innovations require the use of certain related assets to produce & deliver new products and services - Typically lie downstream & may have other uses - New products and processes can either destroy or enhance the value of these assets ((Tushman, Newman &Romanelli 1986) cited Teece 2008). Example invention of disc brakes rendered drum brake technology investment next to useless • **Financial Assets** - Cash position & degree of firm's leverage may have strategic implications, particularly when short term responsiveness to opportunities is enhanced • **Reputational Assets** - Reputations shape the responses of customers, suppliers & competitors - Due to the imperfect nature of reputation, perception is often more important than the true state of affairs with a firm. • **Structural Assets** - Formal & informal structures have an important bearing on the rate & direction of innovation & how competences & capabilities co-evolve ((Argyres 1995) cited Teece 2008) - Degree of hierarchy, vertical & lateral integration are important elements - Distinctive governance modes , e.g. high flex, multi-product, virtual corporation, integrated firms, integrated structures work better for systemic innovations • **Institutional Assets** - Regulatory systems, intellectual property regimes, anti-trust laws, higher education & national culture are critical elements of the business environment - May not be firm specific - Geographic location may influence importance ((Nelson 1994) cited Teece 2008)

	• **Market (structure) Assets** - Product market position matters, but not the overall determinant of the fundamental position of the organisation in its external environment • **Organisational Boundaries** - Degree of industry integration (vertical, lateral & horizontal) is significant - Hierarchical structures may work better than arms length contracts when specific assets or intellectual capital are at issue
Paths	• **Path Dependencies** - A firms previous investments & routines constrain its future behaviour - Amplified by 'increasing returns to adoption' ((Nelson 1996& Rosenberg 1982) cited Teece 2010) - Early leads won by good luck or special circumstance can also become amplified by increasing returns ((Arthur 1983) &(Mitchell 1989) cited Teece 2008) In some cases organisations controlling complimentary assets may start last but finish first - Balance between switching costs & switching benefits may create lock-in • **Technological Opportunities** - Prior research activities impact the breadth & depth of options & the amount & level of R&D the firm can justify - Prior research activities condition the firm's management to be able to perceive alternatives

Source: Table developed for the project based on characteristics identified by Teece (2008, p.33-43).

Key lessons

To maximise the benefits of the *XYZ* SWOT and dynamic capabilities analysis, it was necessary to develop an action plan that aligned the *XYZ* cyber strategy initiative with its overall strategy to leverage its resource strengths, take advantage of market opportunities, and correct or minimise resource deficiencies within the schoolwhilst preventing external threats (Thompson et al. 2008). Six core recommended actions for *XYZ* are detailed below.

Aligning strategy. Review organisation processes to assess their alignment with the *XYZ* vision mission and strategy. A holistic approach, aligning other organisation processes such as development plans, performance measurement and rewards to support strategy can contribute to improved organisation performance (Aguinis 2009). When processes and structures are aligned with strategy they support the achievement of strategy by eliminating barriers to effective strategy execution (Thompson et al. 2008).

Leveraging strengths. Document a management case study of the key activities and events. This would lead to successful and timely identification of cyber safety as an emerging strategic opportunity which would be positively communicated by *XYZ* senior executives and academic leaders at planning and other relevant management events. This would embed the case study story into *XYZ's* organisation culture and create a shared understanding of how success was achieved, which in turn would encourage continued identification of future opportunities. Aligning an organisation's culture with strategic initiatives is one of the most critical internal factors when implementing strategic change and a critical factor in promoting innovation (Hanson et al. 2011).

Formalise processes to identify and develop opportunities to exploit the learning curve expertise gained during the cyber safety initiative into other client service needs. There is the potential for learning from the action itself by conducting 'after action reviews' at the completion of major initiatives (Yorks 2005). These reviews would include supporting 'idea champions' who identify and develop emerging strategies or innovations, and recognising all attempts as successes. The latter would include the timely abandonment of strategies that do not meet criteria since they also provide learning opportunities for the organisation (Rothwell 2005).

Actively pursue varied IT supplier relationships to continue exploiting 'first to market' opportunities for IT innovations. This occurred in the past on an *ad hoc* basis, for example *XYZ* partnered with Microsoft on their early adoption program to deploy Windows 7 prior to the launch date.

Promote the adoption of a code of conduct for IT professionals working in private and state schools, enhancing the school's innovative reputation. A 'first to market' strategy only becomes a sustainable competitive advantage when it is supported by a pattern of continuous improvement over time generating a reputation of innovation (Hanson et al. 2011).

Exploiting opportunities. Develop other school social policy opportunities. For example *XYZ* has already flagged other *XYZ* policy initiatives, 'Safe Partying' and 'Drug Policy', as examples of potential parent support opportunities that *XYZ* could develop to meet a broader range of client needs. Relatedly, they could pursue the development of a code of conduct and 'cyber alert' system with Australian private school associations to promote excellence in reporting and handling of cyber issues. This would further enhance *XYZ's* reputational assets, one of their sources of sustainable competitive advantage.

Correcting deficiencies. Develop extensive documentation to support cyber initiative. This would include defining stakeholder roles, expectations and consequences, policies and procedures based on behavioural studies and *XYZ* experience, and support materials for behavioural and cyber skills development for staff development. In keeping with the cyber initiative this material could be delivered to staff using multiple training modes including self directed e-learning (Yorks 2005).

Similarly, develop a communication strategy which utilises multiple sources of communication to engage and address the specific needs of each key stakeholder group, identify and remove barriers to communication and put in place processes to monitor that information being sent is fully understood (Kerzner 2009). *XYZ's* communication is often limited to emails, newsletters and opportunities such as year 7 transition meetings and notebook information evenings. Face to face events involving students and parents were not exploited. Communication is a vital step in gaining the acceptance of change in any organisation (Schultz 1991).

Plan and implement the framework for a knowledge management system. Such a process would ensure the currency of the cyber safety website and manage the efficient flow of information from all sources into the website and effectively share the collective knowledge of teachers, ICT staff, external experts, parents and students. Information and knowledge

refers to all areas of cyber safety including procedural and policy information, website updates and alerts, behavioural processes, case studies, and staff development resources including academic and educational studies of cyber behaviours.

Effectively sharing collective knowledge extends beyond just repeating the stories; it involves creating a learning culture. This has been referred to as moving from individuals 'learning-in-organisation' to 'learning-by-organisation' where individual-level learning results in changes that are captured and widely utilised by the organisation, including informal norms, or changes that are codified in formal procedures or practices (Yorks 2005). There is a political element to changing the learning environment because such changes often impact people and work units who have benefited from the current configuration of practices, therefore involvement and engagement of staff is critical to creating change (Yorks 2005).

Finally, implement a project management methodology for all significant *XYZ* projects and throughout the ICT function. Simple procedures such as formalising project scope, objectives, and communication strategy and success measures would greatly improve the likelihood of *XYZ's* projects successfully meeting both internal and external client needs. A more fluid matrix reporting structure for ICT to support the provision of services that meets the needs of its internal academic clients could be developed. The current functional organisation structure does not support the integration and development of ICT projects that meet academic client needs as reported in the Stage 4 analysis findings. Functional structures are most appropriate in stable, predictable environments; effective cross-unit collaboration is usually needed to build competitive capabilities in strategically important activities (Thompson et al. 2008). A matrix reporting structure may be more effective in matching the dynamic technology environment to the academic needs of *XYZ* (Noe et al. 2008, Kerzner 2009).

Eliminating or minimising threats. Review and improve risk management procedures for *XYZ* projects involving external publicity campaigns. All *XYZ* employees should be

responsible for managing risk, and processes for risk recognition and assessment of the appropriate risk strategy should be required for all *XYZ* projects (Cowan 2004).

Future applications. The final recommendation is that the SWOT and Dynamic Capabilities Framework should continue to be used.The SWOT analysiswhencombined with the Dynamic Capabilities Framework provided an effective way of identifying the strategic opportunities of *XYZ*that are most likely to lead to a sustainable competitive advantage. This procedure has applications for other organisations making strategic decisions between competing opportunities, such as 'buy or make' decisions, because applying the Dynamic Capabilities Framework to the SWOT provides a means of allocating scarce resources to the opportunity most likely to achieve sustainable competitive advantage (Teece 2008).

Conclusion

In summary, this research study, using a SWOT analysis and Dynamic Capabilities Framework, has provided *XYZ* with a refined list of priorities linked to potential sources of sustainable competitive advantage. It is not practical for *XYZ* to immediately implement all the recommended actions listed in the key lessons of this report. Nevertheless, the research has provided *XYZ* with a clear direction to move the scarce resources and focus of the cyber safety initiative away from the 'community-service' website focus, which has little long term sustainable competitive advantage, toward a focus on the development of excellence in the behavioural policy and process aspects of the *XYZ* cyber support service. The CEO of The Alannah and Madeline Foundation echoes this conclusion (Slocombe 2011):

> *It is important to remember that this is an issue of behaviour, more than it is of technology.We really need to get serious about behaviour and support schools to focus on building a culture of respect and caring in addition to teaching the traditional academic subjects.*

References

Aguinis, H 2009, *Performance Management* 2nd ed, Pearson Education Inc. New Jersey, U.S.A.

Anonymous 2010, *What's the Government Doing About Cyber Safety?* Family- School & Community Partnerships Bureau, Australia viewed 27 July 2010, <www.familyschool.org.au/2010/06/whats-the-government-doing-about-cyber-safety/>.

Australian Communications and Media Authority 2011, 'Consequences of creating sharing or accessing inappropriate online content,' *Australian Communication and Media Authority*, viewed 1 February 2011, <http://www.cybersmart.gov.au/Schools/Common%20cybersafety%20issues/Inappropriate%20content/Consequences%20of%20creating%20sharing%20or%20accessing%20inappropriate%20online%20content.aspx>.

Cowan, N 2004, *Corporate Governance That Works,* Prentice Hall, Jurong, Singapore.

Djakovac, L 2009, 'Bullying',*School Post(Term 3)*, South Australian Association of State Schools Organisation, viewed 27 July 2010, <www.saasso.asn.au/media/files/7682.pdf>.

Dyson, RG & O'Brien, FA 1998, *Strategic Development: Methods and Models,* John Wiley & Sons Ltd, Chichester, West Sussex, England.

Gillard, J 2010, 'National pilot to increase cybersafety in schools', *Ministers Media Centre,* Canberra, ACT, Australia, viewed 27 July 2010 <www.deewr.gov.au/ministers/gillard/media/releases/pages/article_100210_131616>.

Hanewald, R 2008, 'Confronting the pedagogical challenge of cyber safety', *Australian Journal of Teacher Education, 33* (3), pp.14-15.

Hanson, D, Hitt, MA, Ireland, RD, Hoskisson, RE 2011, *Strategic Management: Competitiveness and Globalisation,* 4th edn, Cengage Learning Australia Pty Limited,South Melbourne.

Kaiser, M 2010, 'Cybersecurity, safety and ethics education falls short in U.S. schools', *U.S. Newswire,* Washington D.C., Washington, U.S.A, viewed 18 August 2010, <URL:http://proquest.umi.com/pqdweb?did=1970394551&sid=1&Fmt=3&clientld=20831&RQT=309&VName=PQD>.

Kerzner, H2009, *Project Management: A Systems Approach to Planning Scheduling and Controlling,* 10th edn, John Wiley & Sons Inc, New Jersey.

McLean, S 2009, 'Submission 55 Legislative Council General Purpose Standing Committee No 2: Inquiry into bullying of children and young people',*Legislative Council General PurposeStanding Committee No 2,* Canberra, ACT, Australia, viewed 30 October 2010, <www.cybersafetysolutions.com>.

McGrath, H 2009, *Young People and Technology: A Review of the Current Literature*, 2nd Edition,School of Education, RMIT University,The Alannah and Madeline Foundation, Melbourne, Victoria, Australia, viewed 27 July 2010,<www.amf.org.au/cybesafety/>.

Mason, M 2010, 'Sample size and saturation in PhD studies using qualitative interviews', *Forum Qualitative Science Research*, vol. 11, no. 3, art. 8, viewed 18 July 2010, <http://www.qualitative-research.net/index.php/fqs/article/viewArticle/1428/3027>.

National Cyber Security Alliance 2009, 'National cyberethics, cybersafety, Cybersecurity Baseline Study 2008',*National Cyber Security Alliance,* viewed 30 October 2010, <http://www.staysafeonline.org>.

National Cyber Security Alliance, Educational Technology Policy, Research and Outreach,Microsoft Corporation and Zogby International, 2010, 'The State of K-12 Cyberethics, Cybersafety and CybersecurityCurriculum in the United States',*Staysafeonline,*viewed 30 October 2010, <2010 The State of K-12 Cyberethics, Cybersafetyand Cybersecurity Curriculum in the United States, <http://www.staysafeonline.org>

Noe, R, Hollenbeck, J,Gerhart, B & Wright, P2008, *Human Resource Management: Gaining A Competitive Advantage,* 6th edn,Mc Graw Hill Inc, New York, U.S.A.

Porter, M 1985, *Competitive Advantage: Creating And Sustaining Superior Performance,* 1st edn, The Free Press, New York, New York, U.S.A.

Rice, JL, Martin, NJ, Carpenter, MA & Sanders, WG 2010, *Strategic Management: A Dynamic Perspective: Concepts and Cases,* 1st edn, Pearson Australia Group Pty Ltd, Frenchs Forest, NSW, Australia.

Rothwell, W 2005, *Effective Succession Planning: ensuring leadership continuity and building talent from within,* 3rd edn, AMACOM, New York, U.S.A.

Saunders, M, Lewis, P & Thornhill, A2009, *Research Methods for Business Students,* 5th edn, Pearson Education Limited, Harlow, Essex, England.

Schultz, C 1991, 'Managing change in the public sector: acase study', MBA thesis, Melbourne University, Melbourne, Australia.

Slocombe, DJ viewed 17 January 2011, http://www.amf.org.au/Cybersafety/.

Smith, PAC & Day, A 2000, 'Strategic planning as action learning',*Organisations and People, v*ol. 7, no. 1, pp. 1-14.

Stonehouse, G & Pemberton, J 2002, 'Strategic planning in SME's - some empirical findings',*Management Decision, v*ol. 40, no. 9, pp. 853-861.

Teece, D2008, *Technological Know-How, Organizational Capabilities, and Strategic Management: Business strategy and enterprise development in competitive environments,* 1st edn, World Scientific Publishing Co.Pte. Ltd, Singapore, Singapore.

The Age 2010, 'Digging up dirt to salvage a cyber reputation',*The Age,* Melbourne, Victoria, Australia, viewed 12 January 2011, http://www.theage.com.au/technology/technology-news/digging-up-dirt-to-salvage-a-cyber-reputation-20100827-13vyj.html.

The Alannah and Madeline Foundation 2010, 'Media Release: The Alannah and Madeline Foundation: Media Conference Outcomes', *MediaNet Press Release Wire*, Sydney, NSW, Australia, viewed 18 August 2010,http://proquest.umi.com/pqdweb?did=2006810761&sid=1&Fmt=3clientld=20831&RQT=309&VName=PQD.

Thompson, A, Strickland, A and Gamble, J 2008, *Crafting and Executing Strategy: The Quest for Competitive Advantage,* 16th edn, McGraw-Hill/Irwin, New York, New York, USA.

Yin, RK 2008, *Case Study Research*, Sage, London, England.

Yorks, L 2005, *Strategic Human Resource Development,* 1st edn, South Western College Publishing, Mason, Ohio, USA.