Strategic Planning for Secure Digital Transformation: A Socio-Technical Approach

Martin Koch[0000-0002-6679-6350], Kent Illemann, Daniel Riddarvinge

"[Strategic Planning] is not a box of tricks, a bundle of techniques. It is analytical thinking and commitment of resources to action. Many techniques may be used in the process – but, then again, none may be needed." *(Drucker, 1973,1974)*

Abstract. Keeping the enterprise secure is increasingly becoming a key strategic priority for top executives. Recent high-profile cyber breaches and leaked customer data has shown that failure to understand cyber security at a strategic level can lead to severe consequences. Digital transformation of core business models is fueling this as well, both by increased value of digital assets and by increased number of connections to external partners or customers using self-service channels. To enable security to be included in the strategic planning there is a need to replace traditional prescriptive and often internally focused technological assessment models with a descriptive socio-technical perspective. High level strategic decision-making can then be based on analyzing the internal security strength and weaknesses compared with external opportunities and threats using a S.W.O.T. analysis. As a result, a main security strategy can be shaped around one of four main strategic options; minimizing external threats and internal weaknesses combined with taking advantage of the internal strengths and external opportunities that are identified using a socio-technical maturity model.

***Keywords*:** Socio-Technical Modelling, Strategic Planning, Security, IT-Security, SWOT, TOWS, Capability Maturity Model, CMM

1 The Socio-Technical Digital Transformation Design Approach for Security

The socio-technical approach is adding a broad perspective to security including not only technical solutions and external risks, but also taking the social factors of security into consideration (Kowalski, 1994). Peoples ability to understand and accept the additional complexity driven by security is increasingly vital to the enterprise:

"The capacity of people to deal with technical and organizational complexity and find meaning and satisfaction working in these systems lags the capacity of organizations to create digitally enabled work systems that technically should work—if only humans can be trained to understand, embrace, and be able to operate effectively and thrive within them" (Scheiber, 2017)

Digital transformation of business is driving the appearance of new threats to the enterprise. Security can no longer be perceived as protecting assets from the outside, since tight interdependence across multiple complex entities blurs the border between what is inside and what should be kept outside:

"The tight technical interdependence across complex organizations means that errors in one location may cause service disruptions, delays, and even shut-downs in others" (Kerstetter, 2017)

The digital socio-technical design approach (Winby & Albers Mohrman, 2018) is suggesting adding strategic planning tools to the socio-technical design model in order to create a strategy driven approach. From a security perspective, this would imply an approach with the combination of a well-known socio-technical security model combined with a commonly used tool for strategic planning.

2 Selecting the model and tools

There are many alternative tools and models that could be used for a digital socio-technical security approach. It is outside of scope of this paper to find the optimal combination but as guidance the following adapted the S.M.A.R.T. checklist for Goals (Doran, 1981) summarizes the "design criteria" used:

Area	Design Criteria
(S)pecific	Well known. Selecting model and tool with accepted use and terminology.
(M)easurable	Results should be easily qualifiable and comparable.
(A)chiavable	Ease of use. Understandable across a wide set of audience with disparate background, not drawing unnecessary attention from the subject.

Area	Design Criteria
(R)ealistic	The models should not claim to prescribe or control but aim for strategic guidance, influence and support understanding.
(T)imely	To quote Sheryl Sandberg "Done is better than perfect". Quick turn-around time to a useful result.

Table 1. SMART Design criteria for model selection

3 The use of a Capability Maturity Model (CMM)

The Capability Maturity Model (CMM) was first described by Humphrey (Humphrey, et al., 1987) using five different maturity levels. The work is generally perceived as originating from Nolan's stage theory (Nolan, 1973). The model has recently gained popularity with usage in several international standards (ISO/IEC, u.d.) and adaptions by commercial actors like ISACA (ISACA, 2012), its subsidiary CMMI Institute (CMMI Institute, 2019) among others. A Google search on the term "Capability Maturity Model" results in more than 26MM hits. (April 2019)

Maturity models can be both descriptive and prescriptive (Berghaus & Back, 2016). In Cobit 5 (ISACA, 2012) the model used both to describe the current status of the enterprise and later to set a desired target level (and track changes). Note that the highest level is not always the desired one due to high cost compared with reduced risk.

Example of maturity levels for process maturity with an additional level "0" for non-existing (ISACA, 2012):

Maturity Level	Name
0	Non-existent
1	Ad-hoc
2	Repeatable
3	Defined Process
4	Managed and Measurable
5	Optimized

Table 2. Maturity Levels in Cobit 5

To conclude, the CMM is one of the most widely used models to measure and prescribe maturity in general and particularly in IT and IT-related processes.

SWOT Analysis and TOWS Strategies as a Tool for Strategic Planning

The SWOT Analysis is "[…] a useful tool for reviewing a firm's competitive position." (Sammut-Bonnici & Galea, 2014) and consist of a simple 4-box matrix to assess the enterprise internal (S)trength, (W)eakness and external (O)pportunities, (T)hreats. The model has no official creator but is generally known to be first used by the SRI International in the 1960-70 (Humphrey, 2005). A Google search on "SWOT Analysis" gives over 48MM hits (April 2019).

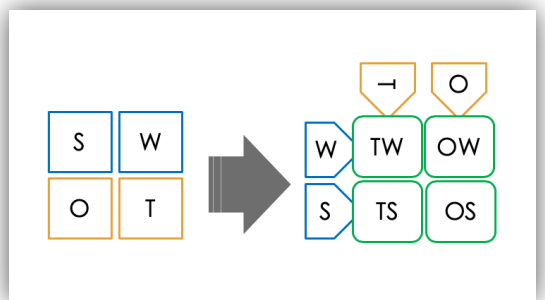

Fig. 1. The SWOT matrix and the four related main strategies

The TOWS matrix (Weihrich, 1982) creates a suggested path from the SWOT analysis to a generic set of four main business strategies:

Strategy	Comment
WT Strategy (mini-mini)	Focusing on the weakness of the organization and the treats. This is an avoidance strategy. Use as a core strategy for a business it typically results in merger or liquidation since being in business is taking risk.
WO Strategy (mini-maxi)	Focusing on the opportunities in the market by quickly acquiring capabilities either by acquisition or internal build up.
ST Strategy (maxi-mini)	Focusing on using the company strength to reduce an external threat. This could be by using an internal R&D knowledge to prepare for a shift in the market, replacing a current product.
SO Strategy (maxi-maxi)	Focus on maximizing existing strength to (continue) to harvest a market opportunity. Sometimes referred to as a "Fat Cat" strategy.

Table 3. The four principal TOWS strategies

The SWOT and accompanying TOWS model continues to be very popular and practitioners favor it since it is easy to explain and use to a wide set of audience when taking a collaborative approach to strategy (Seebohm, 2014).

Our proposed Combined Approach

A Socio-Technical Capability Model

We propose a CMM that use dimensions that covers both social and technological aspects of security. As an example, we have created dimensions based on various best practice including SBC (Kowalski, 1994). The below table shows these dimensions and some sample questions for illustration:

Dimension	Sample Questions
Cultural	• Does the company understand the culture in the country? • Does the company promote the company culture? • Is there a company "Code of conduct" and how is it promoted?
Legal	• Does the company see regulation as a business driver or a business inhibitor? • Does the company see the regulations as risks or opportunities? • Does the company make money on laws and regulations?
Compliance	• Is there a policy for information security? • Is there a policy for Architecture? • Is there a policy for Code of Conduct?
Operations	• Is the operational management based on ITIL or other frameworks? • Is operational management part of company strategy? • Are there routines for recovery?
Technology	• Are there automated controls over computers and software used? • Is there automated backup and restore of our information? • Are there technical installations to protect our data?

Table 4. Sample questions defining dimensions of the CMM

A SWOT Analysis comparing with Competitors and a Baseline

The SWOT analysis has two different perspectives:

- Internal state of the socio-technical security posture
- Competitors (perceived) position

The SWOT model implicitly assumes that one is stronger or weaker compared to a baseline. The analysis can be done without explicitly describing this the baseline, but with the risk for tacit bias. By explicitly stating the baseline the purpose of the SWOT is more clearly described. Example of baselines that could be used would be external cyber threat capabilities or customers/users' general expectations on security capability.

Based on the result of the CMM assessment, the SWOT can be populated.

Area	Relationship
(S)trength	When the internal socio-technical security posture is stronger than the competitors.
(W)eakness	When the internal socio-technical security posture is weaker than the competitors.
(O)pportunity	When the baseline is lower than the internal socio-technical security posture.
(T)hreat	When the baseline is higher than the internal socio-technical security posture.

Table 5. Conversion of CMM to SWOT

The SWOT is then converted to generic TOWS strategies for security. Note that depending on the choice of baseline and CMM dimensions the specific strategy will look different.

Strategy	Comment
WT Strategy (mini-mini)	Security strategy focusing decisions on minimize weakness and threats. (This is probably the most common security strategy)
WO Strategy (mini-maxi)	Security strategy minimizing weakness and focusing on security related opportunities.
ST Strategy (maxi-mini)	Security strategy leveraging existing strength and focus on external threats.
SO Strategy (maxi-maxi)	Security strategy leveraging existing strength and focus on external security related opportunities.

Table 6. Fig. **2.** Four main generic security strategies according to TOWS

References

1. Berghaus, S. & Back, A., 2016. Stages in Digital Business Transformation: Results of an Empirical Maturity Study. s.l., MCIS, p. 3.
2. CMMI Institute, 2019. *CMMI Institute home page.* [Online] Available at: https://cmmiinstitute.com/ [Accessed 2 April 2019].
3. Doran, G. T., 1981. There's a S.M.A.R.T. Way to Write Management's Goals and Objectives. *Management Review*, 70(11 (AMA Forum)), pp. 35-36.
4. Drucker, P. F., 1973,1974. *Management: Tasks, Responsibilities, Practices.* New York(NU): HarperCollins Publisers.
5. Humphrey, A. S., 2005. SWOT Analysis for Management Consulting. *SRI Alumni Association Newsletter*, December, pp. 7-8.
6. Humphrey, W. et al., 1987. A method for assessing the software engineering capability of contractors, s.l.: Carnegie Mellon University.
7. ISACA, 2012. A Business Framework for the Governance and Management of Enterprise IT. In: ROLLING MEADOWS: ISA, pp. 41-45.
8. ISO/IEC, n.d. *ISO/IEC 15504,21827,* s.l.: s.n.
9. Kerstetter, J., 2017. *New York Times.* [Online] Available at: https://mobile.nytimes.com/2017/03/13/technology/tech- roundup-amazon-error-is-a-reminder-that-no-company-is-infallible.html [Accessed 3 April 2019].
10. Kowalski, S., 1994. IT Insecurity: A Multi-disiplinary Inquiry, Stockholm: s.n.
11. Nolan, R., 1973. Managing the computer resource: A stage hypothesis.. *Communication of the ACM,* 16(7).
12. Sammut-Bonnici, T. & Galea, D., 2014. SWOT analysis. In: *Wiley Encyclopedia of Management.* s.l.:John Wiley & Sons, Ltd..
13. Scheiber, N., 2017. *How Uber usus psychological tricks to push drivers' buttons.* [Online] Available at: https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html [Accessed 3 April 2019].
14. Seebohm, L., 2014. Collaborative Tools for Strategic Line Planning. s.l., Concurrent Strategies.
15. Weihrich, H., 1982. The TOWS Matrix a Tool for Situational Analysis. *Long Rage Planning,* 15(2), pp. 54-66.
16. Winby, S. & Albers Mohrman, S., 2018. Digital Sociotechnical Systems Design. *The Journal of Applied Behavioural Science*, Volume 54(4), pp. 399-423.