Porters' Elements for a Business Information Security Strategy

Yuri Bobbert is professor at LOI University of Applied Sciences (The Netherlands) and Ph.D. researcher at Antwerp University (Belgium) in the field of business information security governance and management. Bobbert is also nonexecutive director of DPA|B-Able, a security governance consulting firm. In 2010, Bobbert published *Maturing Business Information Security (MBIS)*, a framework to establish the desired state of security maturity. In 2015, Bobbert will publish his book *How Safe Is My 'Share'?*

Hackers and negative social media hypes have proven able to bring proud organizations to their knees, yet many information and communications technology (ICT) security managers lack a strategy to anticipate and overcome such unpredictable challenges. A survey conducted among key people in the ICT security field reveals how perilously far behind their strategic thinking has fallen and what managers and board members can do to catch up.

The unforeseen risk in new media today can hardly be overstated. A burglary at the San Diego (California, USA) headquarters of Impairment Resources LLC, resulted in the leak of 14,000 patients' medical records and the bankruptcy of the company in 2012.[1] Last year, the Dow Jones Industrial Average dropped 143 points after hackers broke into the Twitter feed of the Associated Press and sent a false message saying US President Barack Obama had been injured in a White House explosion.[2] Dutch certificate authority DigiNotar was hacked in 2011[3] with fraudulent certificates issued in the company's name. The company lost its government contract, and within three months, it went bankrupt.

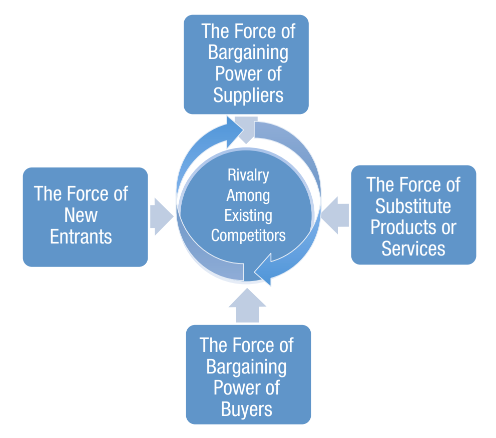
Despite such clear and present dangers, ICT security managers remain ill-equipped for future incidents. This is reinforced by an April 2013 study conducted by B-Able, a Netherlands-based consultancy, in cooperation with the University of Antwerp Management School (Belgium). Forty-one experienced ICT security managers, all of whom have worked for 10 years or more in the field, were asked a range of questions about the forces they deal with when formulating their security strategy.

SURVEY DETAILS

The questions within the survey were based on Michael Porter's Five Forces analysis.[4] Porter's Five Forces are a commonly used tool to analyze how attractive an industry is. Porter distinguishes (**figure 1**):

1. Competition from rival sellers
2. Competition from potential new entrants
3. Competition from substitute products producers
4. Supplier bargaining power
5. Customer bargaining power

Figure 1—Porter's Five Forces


The Force of Bargaining Power of Suppliers
The Force of New Entrants
Rivalry Among Existing Competitors
The Force of Substitute Products or Services
The Force of Bargaining Power of Buyers

Based on: Michael Porter's Five Forces

This model can be used as a frame of reference to examine numerous forces a security professional can address when establishing a "security strategy."

In the survey, managers were asked whether the various forces they faced were dynamic or static in nature and whether the managers felt able to bend these forces to their strategic advantage. The results were used to compile a list of suggestions meant to help managers develop a more robust strategy.[5]

The results were sobering. Two-thirds of the forces ICT security managers said they face are dynamic. In other words, they are unpredictable factors such as intellectual property theft, extortion, hacking, social media rumors gone wild and other new-technology phenomena. Only one-third of the forces they deal with are static, such as compliance legislation, ISO standards and mandatory audits. Of respondents, 58 percent consider it important to address these external forces in their strategy formulation in the future. Since they had not done this up until the survey, the survey results show ICT security managers focus their strategy on the more predictable, recurrent forces (compliance-related), rather than on the more plentiful and potentially more damaging forces.

BLIND SPOT

It is not as if ICT security managers are naive. They are not. In response to the survey, in fact, they overwhelmingly indicated that supply chain risk management (e.g., cascade failures due to overlooked forces) should be one of the highest priorities in their organization. So they understand they have a blind spot preventing them from anticipating risk. But knowing that is not enough. The survey showed that managers are poorly informed about the specific dangers they face and the potential impact of dynamic forces, much less about how they should respond in the event of a full-blown crisis. Of respondents, 78 percent said they poorly or fairly influence these forces once they impinge. An example of this can be seen through the April 2013 distributed denial-of-service (DDoS) attack that paralyzed ING Bank, a global financial institution based in The Netherlands. The incident slashed shareholder value and a flurry of criticism via social media cost ING customers.[6] If the bank had understood and respected the power of such dynamic forces—in this case, uncensored social media caused confusion[7]—and been transparent about the attack, the damage could have been limited. Instead, ING denied the seriousness of the attack, evaded questions and remained silent for far too long,[8] allowing the conversation on Twitter to proliferate and leave the lasting impression that the bank had failed to respond. This incident, in addition to many others,[9] reveals a lack of preparedness—a gaping hole in the ICT security strategy that is all too common.

Positive exceptions are observed now and then, at least in terms of crisis management. A good recent example is how a Dutch hospital, Het Groene Hart Ziekenhuis, responded when it was hacked in October 2012.[10] Upon discovery that thousands of patients' medical details had been leaked, the hospital immediately responded to the media and notified other stakeholders. Management wasted no time in admitting they had a problem and swiftly followed up with preventive measures so the leak could not recur. The hospital's candid response profoundly influenced the tone of the ensuing (social) media debate, leading to more favorable public perception in the long term.

CONTAINING VS. AVERTING DAMAGE

Surely, though, it would be better if organizations averted such a crisis in the first place. By the time it was discovered that Impairment Resources had lost control of medical records belonging to the roughly 600 insurance companies it served, the damage was done. The lawsuits quickly piled up and no amount of transparency could have stopped the company's impending demise.[11] So an ounce of prevention is worth a pound of cure.

Businesses need to develop an overall business strategy in which ICT security is truly integrated, employing two of Michael Porter's management frameworks: the Five Forces analysis[12] and the value chain. It has been shown how the Five Forces can be subdivided into dynamic and static forces and how inadequate ICT security strategy is, with its inordinate focus on static forces. The second important concept that should be borrowed from Porter is the value chain. And here too, according to the survey findings, ICT security misses the mark, typically focusing on individual activities of the organization rather than considering the role each activity plays in the wider picture. For instance, security specialists see that their business has relationships with third parties, but seldom recognizes these parties as potentially influential forces.

Understanding the value chain and the five forces is a prerequisite for business success.[13] Yet, surprisingly, Porter's frameworks have yet to take hold in the ICT security field.

The top five forces of which ICT security managers say they recognize the impact are:

1. Legislation—95 percent
2. Inspection and supervisory agencies—88 percent
3. Law enforcement (district attorney and police)—69 percent
4. Partners in the (digital) chain (e.g., freight forwarders, Internet service providers, payment handlers)—64 percent
5. Public opinion—60 percent

The top five forces of which ICT security managers say they do not recognize the impact are:

1. Trade unions—79 percent
2. Social media (uncensored reporting)—57 percent
3. Criminals—48 percent
4. Customers—48 percent
5. Suppliers—43 percent

It is too easy to say that organizations simply need to get a grasp on the dynamic forces in the chain and all their problems will be solved. However, the problem is that very few management tools, steering mechanisms or key performance indicators (KPIs) are available to deal with these forces.

Dynamic forces can have major consequences. A surprising 71 percent of experts surveyed indicated that these forces are critical to their business and security strategy. They require the attention of every manager, board member and shareholder. This research shows that strategies based on an awareness of value chains and the five forces can help organizational leaders to:

- Heighten preparedness for unforeseen influences
- Better identify risk and establish the organization's risk appetite
- Anticipate crises and remain in control of strategy

The top five elements for business information security strategy, according to the survey, are:

1. **Stakeholder approach**—When developing a strategy, involve the board of directors (BoD), management, business and all external stakeholders in the chain. Know the KPIs, stakeholder expectations, and how to translate these demands, using the right KPIs, into concrete benchmarks for the organization, management and BoD.
2. **Risk-based approach**—Look at the organization's critical data security in the context of the entire chain. Start by gaining insight into all digital stakeholders and their potential dependencies, weaknesses and risk—both technologically and legally.
3. **Beware the blind spot**—Many forces are dynamic. Ensure the organization is not caught unaware. No one person can stay abreast of every development in this field, so let others update stakeholders on what they do not know.
4. **Do the right things well**—It may seem easier to "learn by doing," but those who prepare a good strategy are less dependent on impromptu solutions.
5. **Integrated organizational process**—Be aware of the chain of forces that influences the organization. Make room for addressing these forces in the strategy and policy plans of the entire organization.

CASE STUDY

A strongly Internet-dependent Dutch business with an annual revenue of €500 million used these elements, Porter's forces, to help it gain a better overview of its stakeholders. The organization realized that it had 266 percent more stakeholders than previously thought. By identifying all 166 digital stakeholders involved in critical business processes and their technical and/or legal dependencies, the organization was able to effectively map out and quantify all risk factors and feed this information back to process owners so risk management could be integrated throughout the organization. This made it easier to specify the knowledge and competencies needed to manage risk and to identify blind spots.

In this case, it became clear that the business lacked the expertise to strategically manage the entire value chain and to set the right KPIs. The organization is currently taking this final step in the process by introducing an integrated dashboard called the SecuriMeter for Governance, Management and Operational Data. The result will be a far stronger businesswide security strategy.

CONCLUSION

The message is simple: Zoom in on specific threats and prepare for them; zoom out and consider the entire context in which the organization operates.

This is not just a lesson for ICT security managers. It can be argued that the most important decision makers in every organization need to take ownership of this problem. "It is imperative that organizations deliver on the promise, or they will soon become irrelevant."[14] Decision makers should give ICT security people a voice in the formulation of overall business strategy. ICT security policy should be made a core aspect of the whole.[15] Only then can an organization consider itself ready to face an uncertain and rapidly changing context and future.[16]

ENDNOTES

[1] Stech, K.; "Burglary Triggers Medical Records Firm's Collapse," Bankruptcy Beat blog, *Wall Street Journal*, 12 March 2012, *http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm%e2%80%99s-collapse/*

[2] Moore, H.; D. Roberts; "AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging," *The Guardian*, 23 April 2013, *www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall*

[3] Prins, R.; "DigiNotar Bancruptcy Public Report," Dutch Government, *Den Haag*, 2011

[4] Porter, M.; "How Competitive Forces Shape Strategy," *Harvard Business Review*, 1979

[5] Porter, M.; "Competitive Advantage: Creating and Sustaining Superior Performance," *Free Press*, 1985

[6] NOS, "Disruptions in Online Banking—377%," 2014, *http://nos.nl/artikel/618846-storingen-online-bankieren-377.html*

[7] RTL Nieuws, "Disruption at ING Caused Hours of Unclearness About Account Balances," 3 April 2013, *www.rtlnieuws.nl/nieuws/storing-ing-urenlang-onduidelijkheid-over-saldos*

[8] Van der Lans, Chantal; "Online Disruptions, Don't Lose Your Customers' Trust," Usability.nl, 10 March 2014, *www.usability.nl/2014/online-storingen-verlies-niet-het-vertrouwen-van-uw-klanten/*

[9] NU.nl, "The Netherlands: Number One in Online Banking Disruptions," 13 January 2014, *www.nu.nl/tech/3674517/internetbankieren-relatief-vaak-getroffen-storingen.html*

[10] NU.nl, "Hospital Regrets Data Breach to the Public" ("Groene Hart Ziekenhuis betuigt spijt voor lek"), 2012, *www.nu.nl/internet/2932335/groene-hart-ziekenhuis-betuigt-spijt-lek.html*

[11] *Op cit*, Stech

[12] *Op cit*, Porter, 1979

[13] McBeath, B.; "Supply Chain Orchestrator—Management of the Federated Business Model in This Second Decade," 2010, *www.clresearch.com*

[14] Stackpole, B. O. E.; *Security Strategy*, Auerbach Publications, USA, 2011

[15] May, C.; "Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy," *Computer Fraud & Security*, iss. 5, UK, 2003, p. 10-13

[16] Sveen, F. T. J. S. J.; "Blind Information Security Strategy," *International Journal of Critical Infrastructure Protection*, Spain, vol. 2, 2009, p. 95-109