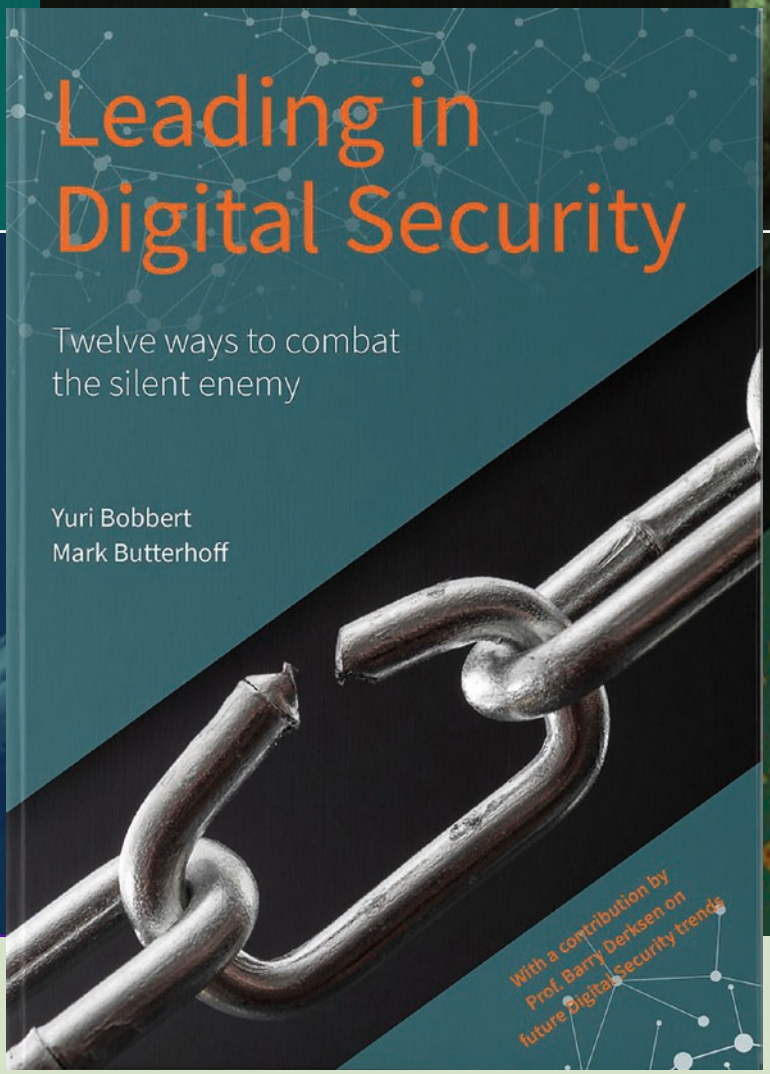
Elly Stroo Cloeck RA RE CIA
is an independent project manager and consultant.
elly@escia.nl

Leading in Digital Security – Yuri Bobbert and Mark Butterhoff



Book review

The biggest security risk at this very moment is ... the human factor, according to *Leading in Digital Security* by Yuri Bobbert and Mark Butterhoff, published in 2020. According to the authors, the weakest link is the end users, who do not follow security instructions, corporate management, who pay too little attention to these risks, and the security professionals themselves, who cannot convey the importance of digital security. High time to fix this, before our brains are in the cloud too!

The book is therefore not about the technology of security but about communication, leadership, culture and all the other things that ensure that security is an integral part of running a business, and not a standalone department. The core of the first chapters is that security professionals need to learn to speak the language of the business and top management. In order to achieve this, a lot of attention is given to well-known management theories with matching jargon.

Of course, practical matters are not lacking, and sufficient attention is given to the (expected) future developments in technology and security. On account of this the book is a sound mix of theory (shaped in management models) and practice, from the authors' personal experiences as well as from research amongst security professionals.

TWELVE WAYS

The book has 6 chapters, leading to "12 ways to combat the silent enemy".

- Chapter 1 is "Leading", and also covers the matrix organisation and high performing teams. I liked the CISO-Capability model, the references to Jim Collins' *Good to Great*, with the Level 5 Executive, and those referring to leadership in the military especially.
- In Chapter 2, "Strategizing", Porter's Five Forces model particularly stands out.
- Chapter 3 is "Changing", in which I was particularly struck by the paragraphs on culture. It explains Boris Groysberg's model, which includes eight values (Learning, Fun, Meaning, Care, Order, Safety, Authority and Results) that can lead to an increase or decrease in staff engagement and customer focus. This chapter also discusses ethics and soft controls.
- Chapter 4, "Governing", amongst other things deals with KPIs and laws and regulations. Lots of examples of KPIs are given, which were collected from security professionals through one of the many surveys that are used in the book. Remarkably however, and also pointed out by the authors themselves, the KPIs are "technocratic" and do not really cover behaviour and culture.
- Then Chapter 5 is about "Funding", covering the business case, customer satisfaction and ROSI: Return On Security Investment.
- Chapter 6, "Trending", reflects the expected trends, from 2120 (so a hundred years from now) back to 2020 ("today and tomorrow"). An excellent chapter that even directly identifies the risks related to hacking. For example, the authors' vision of the future in 2050: nanobots in your body will place your brain "in the cloud", leading to an "Internet of Thoughts". By 2120, our brains will be fully merged with AI and we will be traveling outside our solar system (based on Ray Kurzwell's writings). Fascinating! I must say, the impact of the developments and their associated dangers as depicted in this chapter, make current problems from the previous chapters almost irrelevant. Perhaps you should look upon these as sound exercises?

Each chapter ends with a few key takeaways, which are summarised (again) in the "12 ways to defeat the silent enemy".

IKEA'S TREASURY CHEST

Thus, the contents have many gems, golden tips, and valuable facts. However, this treasury is not placed in a really robust treasury chest. As the sentences were not running smoothly, I realised only later that this is on account of the sometimes literal translation from the Dutch text. On top of that, there are quite a few spelling mistakes. Too bad, because that detracts from the content.

Within the chapters some more structure would have done wonders, many topics are separated without any mutual connection. The many notes at the bottom of the pages are nice, as you don't have to turn to references at the back of the book all the time. In addition, the book is beautifully designed with many pictures and tables in colour and glossy pages (which are sometimes difficult to read in the lamp light).

All in all, it reminds me of an IKEA treasury chest: lots of precious content in a casing that looks nice, is functional, but not robust. Typical DIY. A good editor wouldn't have had any leftover screws ...

INSPIRATION FOR YOUR OWN ACTION PLAN

Overall, I think the authors have done a great job in incorporating so much knowledge into a varied, beautifully executed, and reasonably readable book. It provides a lot of inspiration for your own action plan (do not expect a COBIT-like framework) and that is why it is particularly useful for anyone in an IT / security related management or executive position. The notes and references to other books are extensive, very inviting for a further reading. The topics are very broad, the examples of problems that security professionals run into are recognisable from practice. It effectively holds a mirror up to ourselves, because that silent enemy ... happens to be you?

About the author

Elly Stroo Cloeck RA RE CIA is an independent project manager and consultant. She worked for 20 years as an accountant and IT auditor at KPMG and then as an internal auditor and risk manager at various multinationals. Today, she writes summaries and reviews of management books. Elly can be reached at elly@escia.nl and her website www.1001managementboeken.nl.