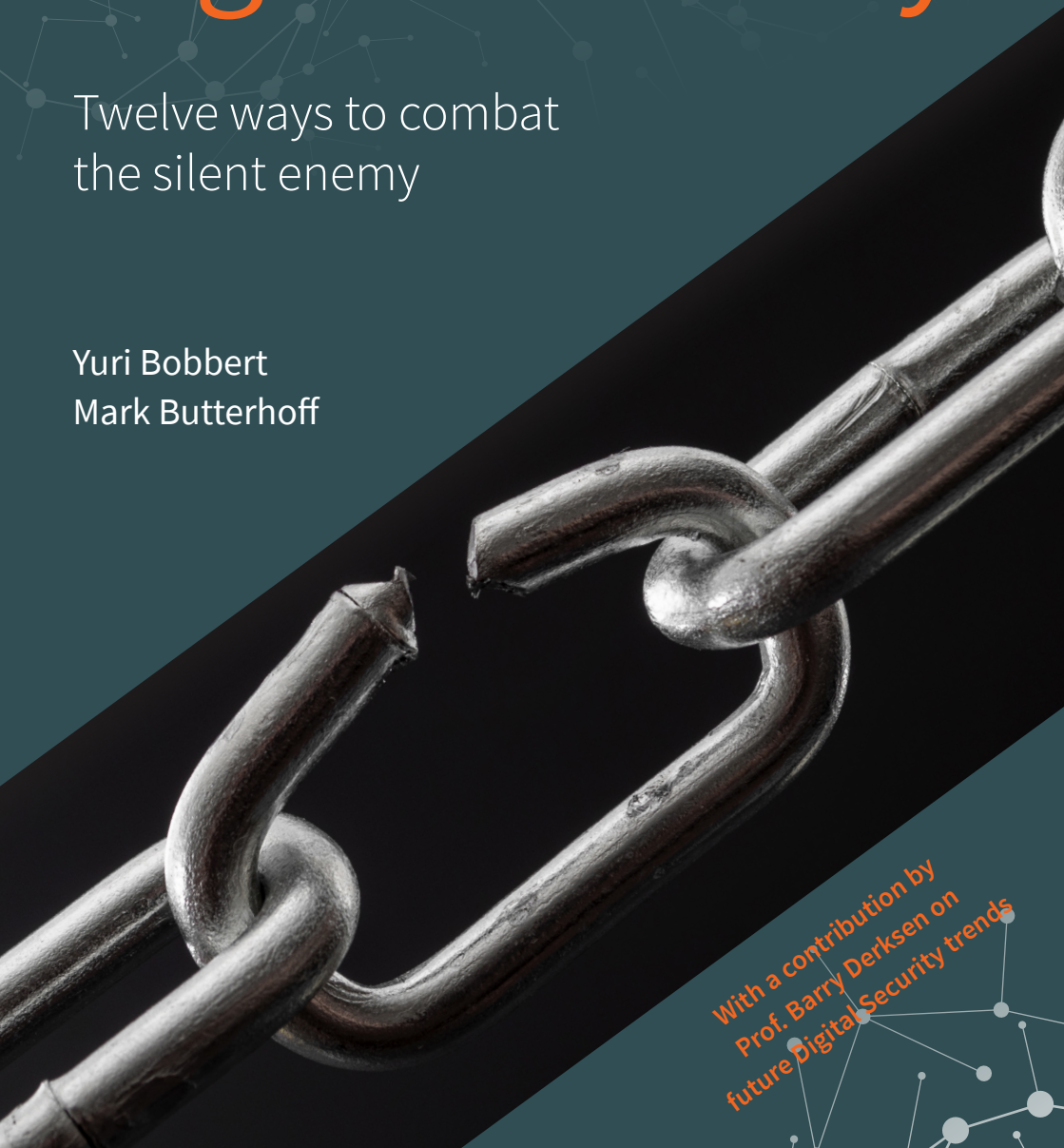
Leading in Digital Security

Twelve ways to combat the silent enemy

Yuri Bobbert
Mark Butterhoff



With a contribution by Prof. Barry Derksen on future Digital Security trends

Leading in Digital Security

Twelve ways to combat the silent enemy

Yuri Bobbert

Mark Butterhoff

With a contribution by Prof. Barry Derksen on future Digital Security trends

More information about this edition can be obtained from www.12ways.net or via info@12ways.net

1st edition	August 2020
Authors	Yuri Bobbert
	Mark Butterhoff
Design	Paul Gerlach
Editor	Michael Gould Associates (MGA)
Writing contributions:	Barry Derksen (section Trending) & Ed Lute (Interludes)

ISBN/EAN	9789 0903 35 13
NUR-Code	801
NUR-description	Management: general

Leading in Digital Security

Twelve ways to combat the silent enemy

Yuri Bobbert

Mark Butterhoff

With a contribution by Prof. Barry Derksen on future Digital Security trends

“Good leaders organize and align people around what the team needs to do.
Great leaders motivate and inspire people with why they’re doing it.”

Marillyn Adams Hewson

chairman, ex-president and ex-chief executive officer of the aerospace and defense manufacturing company Lockheed Martin.

Contents

“History teaches us that men and nations behave wisely once they have exhausted all other alternatives.”

Abba Eban (1915-2002)

Israeli Statesman

Preface

Throughout history, the importance of security, to countries and companies, has usually only been understood by finding out the hard way. Only after disasters have occurred do men and nations realize that it would have been wiser to think ahead, invest in security, and avoid catastrophe. Time and time again we have seen naive people running high risks without proper preparation, only to recognize afterwards that most of the damage could have been prevented by basic security measures. As Yuri Bobbert and Mark Butterhoff point out in this book, in the new world of digital security the same old dynamic of learning the hard way is playing out again. This is why they aim to support managers in taking the lead in building digital systems that are capable of fending off the silent enemy before they have exhausted all the other alternatives.

The approach taken by Bobbert and Butterhoff is unique and powerful in three mutually reinforcing ways. First, their approach to digital security is organizational rather than technical. To explain, let me make a short sidestep. If you think about military security, you immediately recognize that some people prefer to talk about the technical side – the hardware such as tanks and ships. While this is not unimportant, every military strategist will tell you that wars are not won by the side with the best hardware, but by those with the best way of organizing themselves and employing the hardware to achieve strategic advantage. If you talk about safety in a factory, again some people will focus on the technical side, such as hardhats and safety railings. Here too the hardware is useful, but safety needs to be organized. Successful companies encourage people to embrace safe working practices, while leaders support this behavior, building a strong safety culture in the process. Bobbert and Butterhoff take the same approach to digital security, acknowledging the importance of technology, but focusing strongly on creating the organizational capability to remain secure.

The second distinguishing characteristic is that Bobbert and Butterhoff's approach is strategic rather than operational. They argue that digital security is not only about operational risks, but also about strategic risks that could sink the whole organization. Just imagine leaving national security to local tank commanders at the border because that's where the problem will first appear, instead of making it the responsibility of the president or prime minister. In the same way, companies that are successful with security will tell you that it needs to be what the German's call a chefsache – on the plate of the CEO, because mistakes can deeply impact the entire organization. Bobbert and Butterhoff argue strongly that digital security needs to be on the strategic agenda of top management and explain how that can be achieved.

The third aspect of the authors' approach, complementing their organizational and strategic perspective, is that they make digital security an organization-wide issue instead of only a topic for the IT department. Of course, it's very attractive for people in the organization to dump digital security responsibility in IT's lap, so that they can focus on their own KPIs and topics they find more engaging. But digital security requires a collective effort and IT can only do so much on its own. Just imagine if politicians were to delegate national security to the military, while at the same time engaging in dangerous foreign policy. In the same way, companies that have made safety departments responsible for safety have found that such delegation allows all others in the organization to ignore safety, as it's the safety department's problem to solve. Bobbert and Butterhoff convincingly argue that, when it comes to digital security, the chain is only as strong as the weakest link, so an organization-wide approach is essential.

Taken together, these three angles – digital security as organizational, strategic, and company-wide – make this book a "must read" for any manager involved in the topic of digital security, which in the digitalizing world basically means almost all of us. So, it's time to put on your seatbelt on and enjoy the ride.

Prof. Ron Meyer

Managing Director, Center for Strategy & Leadership
Professor of Strategic Leadership, TIAS School for Business & Society, Tilburg University
& Antwerp Management School, University of Antwerp

"'Antifragile' is when something is actually strengthened by the knocks."

Nassim Taleb

Introduction

Nowadays it's impossible to imagine business without technology. Most industries are becoming "smarter" and more tech-driven. Ranging from small individual tech initiatives to complete business models with intertwined supply chains. We're seeing smart cities emerge and society is taking a more holistic view of the regulation of such high-tech developments. Not only from a privacy perspective: who collects what, and for which purpose? But also from a cybersecurity perspective: who protects our digital sovereignty and our "digital heritage"? For policymakers and business leaders technology is no longer a domain that is shrouded in mystery; rather it's an essential business discipline that is here to stay, and it's taught at business schools all over the world. It's also a professional discipline that has got the attention of analysts and supervisory boards[1]. However, at the same time, organized crime has arrived on the scene in a big way. Through hacks and denial-of-service attacks, all sorts of malicious actors are infiltrating our 'digital' society. They can easily take advantage of systems that are sloppily built and configured and they frequently use advanced "socially engineering" techniques to trick their way into organizations. Various scams trick people into thinking they have to update their account information by clicking on a link that's provided. By indiscriminately spamming extremely large groups of people, "phishers" can thus gain sensitive financial information from the small percentage (yet large number) of people who are fooled in this (and other) ways.

Did you know that in 2019 every month 590,000 unique malware[2] variants were created and that in 2020 we reached the milestone of 1 billion unique examples of malware created and

1 *In 2017 Boston Consulting Group reported a 150% increase in regulatory agency reports on Cybersecurity and 129% increase in investor research reports compared to 2013. .*

2 *Short for "malicious software," malware designed to damage a computer system.*

targeted at consumers and organizations.[3] Did you know that users are still the weakest link and that malware causes damage estimated at $150 million dollars per cyberincident?[4] Also that spending on cybersecurity is expected to increase globally to $248 billion in 2023[5]? We've all seen many examples of LinkedIn pages that have moved away from regular IT functions toward digital security functions, even though in the past they've never paid much attention to this topic. Nevertheless it's been calculated that the global shortage of security professionals will increase to 3.5 million open positions by 2021.[6]

Once we take a closer look at how the spending on security is spread, we see that most of the money is spent on the more technical part of cybersecurity[7]. Security awareness, i.e. the human factor in information security, seems to be of less importance.

Table 1 Spending on security, taken from Dutch Investments in ICT and cybersecurity

Cybersecurity Submarkets	Value in € Billions		Compound Annual Growth Rate
	2015	2020	
Security services	€13.1	€27.3	16%
Internet of Things security	€6.27	€26.39	33% (up to 55%)
Cybersecurity insurance	€2.3	€7	25%
Cybersecurity awareness training	€0.9	€1.66	13%

When we take a closer look at the providers of information security services, we see not only that the number of cybersecurity companies is growing, but there are also many new startups, with the possibility of being listed on the Nasdaq, and existing large-scale IT providers that now have

3 *Source: https://www.av-test.org/en/statistics/malware/*

4 *According to Ponemon in 2020 the average cost of each data breach will be US$150 million. According to Juniper Research, cybercrime is expected to cost businesses around US$2 trillion dollar. source: https://www.cybintsolutions.com/cyber-security-facts-stats/*

5 *https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#756db286381d / https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/*

6 *https://financesonline.com/cybersecurity-statistics/*

7 *Dutch investments in ICT and Cybersecurity, Putting IT in perspective, The Hague Centre for Strategic Studies, December 2016*

their own security services line of business. For some of them this is the only actual growth market they have, e.g. Atos saw their main growth in Big Data and cybersecurity in 2018[8]. What's particularly interesting is that we've learned that some regular cloud service providers (e.g. Salesforce, Microsoft, etc.). have started delivering paid security services based on data they collect from your company. In other words, you can only access the transactions and user activities created by your employees, or unauthorized individuals, which are stored in "your" cloud service database and event logs if you pay additional fees. Well, at least they present this information to you in a nice dashboard, which they might call their Artificial Intelligence (AI) or machine learning engine.

Although all of these technical security measures and services are necessary within the current connected world, one could ask whether this is their core competence and where their real focus should be. Are these software and services providers actually not like the pharmaceutical companies, which often focus on "managing" diseases rather than treating or preventing them in the first place. Because preventing a disease doesn't allow you to sell more drugs and thus earn more money. Wouldn't it be better within digital security to focus more on the biggest causes of security incidents i.e. the vendors that keep producing technology with basic security flaws? How can it be that we as users, IT staff and security specialists accept that we have to pay more or buy more services to actually get a secure IT/Cloud service that you would expect when buying it, just like in other industries. In aviation, we just had a very tragic experience involving two Boeing 737 MAX airplanes that had a huge impact on the profitability and even the continuity of the entire Boeing company. An error like that in aviation or in the car industry will have a massive impact, but within IT or the Cloud, it appears that the user, IT and security departments are the ones who need to fix an issue caused by the vendor.

8 *Het Financiele Dagblad (Dutch Financial Times), 6 September 2019.*

About the authors

Yuri Bobbert is a scientific tech-leader. He is Chief Information Security Officer at ON2IT and Academic Director / Professor at Antwerp Management School (AMS) Visiting lecturer at the Cyber Security Academy (Leiden University / TU Delft). He has advised more than 300 companies, including NN Group and UWV as Head of Digital Security. Within NN Group he was the Security, Risk and Compliance leader of the Delta Lloyd merger. This is where he met Mark Butterhoff and shared their initial vision and values.
From 2004-2014 Yuri was CEO of a Digital Security advisory and integration company. Yuri holds a double PhD from both the University of Antwerp and Radboud University in the Netherlands and a Master in Business Informatics. His PhD dissertation about "Maturing Business Information Security (MBIS)," describes the managerial side of security and the technology used to measure and administrate it.
His first book was published in 2010 which defines and positions his methods; the second in 2014, describing 25 companies that have applied these methods. In 2018 he published two books: "Critical success factors for effective business information security" and "Cybersecurity in 60 minutes" for Boards and supervisory bodies. Bobbert is co-founder of technologie solutions such as SecuriMeter, SECA/Lockchain and Meetingwizard GSS Software.

Mark Butterhoff has gained experience over the last 20 years in various roles. He has a long history at KPMG, where he worked in information security, IT auditing, and management consulting. After that he worked for several years as program manager and interim manager restructuring and changing mainly IT organizations as well as a post as Interim Chief Information Security Officer. So far he has helped over 80 companies in 17 countries. Alongside his work he also teaches at the TIAS Business School in the Netherlands. Mark has completed studies in various topics, including Business Informatics and IT Auditing.
In 2016 he published a book entitled "Discover the IT Cherry," which describes how to become the most valued IT organization by building trust and creating experiences instead of using the latest technology or implementing new processes. His experiences from work and the insights gained from writing this book were also the basis for writing this book. Solid technology and processes are massively important in cybersecurity; however, they won't help you win the war against this silent enemy. Just as in sports, the army, aviation, healthcare, etc., it's mostly leadership and the people in your organization that make the difference.

Over the years we've seen the digital security profession transformed into an overhyped and fuzzy domain that is often referred to as cybersecurity. Since many authors have written a great deal on this subject in books, journals, and social media blogs, our aim here is to enrich this field with our opinions, viewpoints, and expertise. Thanks to a combined total of forty-five years of experience – experience from our academic backgrounds as well as from our work as security and tech leaders – we are able to focus on things that should work in theory but fail in practice due to all kinds of intangible, "silent" factors. Our intention is not to be exhaustive, nor to criticize others, but to shed fresh light on crucial cyber-related allies, enemies, and issues that are rarely taken into account and talked about, but we believe you should know to help you combat the silent enemy of digital security.

"Security is a complex topic and the authors brought the essentials and the complexity to me in a very understandable, usable and completing style." Very exciting read, especially because the authors wrote the chapters from a practical perspective with a nice balance of academic and creative models. You can apply the "takeaway messages" immediately.

Amir Arooni, Board member and CIO at Discover Financial Services (DFS)

Leading Digital Security offers more than a dozen smart ways to combat the silent enemy; this book – just like Sun Tzu's 'Art of War' – teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; nor on the chance of his not attacking, but rather on the fact that we have made our position unassailable. This book is a "must read" for professionals and students in the field of digital security.

Prof. Hans Mulder, European Research Director of the Standish Group, Boston, USA

In many boardrooms and leadership teams, digital security is a key topic on the agenda. And, considering the rapid digital transformation of our society, its importance will only increase in the years ahead. Boards and leadership teams are aware of the challenges we face, but often seek guidance that is both robust and relevant. The authors of this book have responded to that call by writing a must-read reference guide that connects theories and models to practical instruments and approaches in the field of digital security.

Prof. Steven de Haes, Dean at Antwerp Management School

9 789090 335131 >