Mark Butterhoff
dr. Yuri Bobbert

Digital Security Leadership

Preface by **prof. Ron Meyer**

A CISO Handbook

Teaser

Digital Security Leadership

Mark Butterhoff

Yuri Bobbert

Preface by prof. Ron Meyer

“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

Teaser

Teaser

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

Abba Eban (1915-2002)

Israeli Statesman

Teaser

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.

Teaser

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

Teaser

Teaser

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

Nassim Taleb

Teaser

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.*

Teaser

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

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*

Teaser

the possibility of being listed on the Nasdaq, and existing large-scale IT providers that now have 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.*

Teaser

We all know that the human factor is still the weakest link. Many publications have focused on behavioral and awareness aspects.[9] [10] [11] According to TechDirt, "almost" no one (fewer than 1% of users) reads end-user license agreements (EULAs). Apparently, in an attempt to prove that no one reads these agreements, anti-spyware firm PC Pitstop buried a note in its own EULA, saying they would give $1,000 to the first person who emailed them at a certain address. It only took four months and over 3,000 downloads before someone actually noticed it and sent an email (and got the $1,000). Also, 59% of the employees steal proprietary corporate data when they quit or are fired.

Nowadays, 56% of all mail is spam and this triggers most of the cryptolockers and ransomware. And who said in 2004 that spam will be a thing of the past in two years? That was Bill Gates.[12] According to many publications, users are the weakest link and should therefore also be the main focus for security controls.[13] Often the focus is on end-users clicking on all kinds of vulnerable links in their emails or providing sensitive data to people they shouldn't trust or with whom they are not allowed to share. In our opinion, the human factor also includes those who are actually managing IT systems, information processing facilities and HR. The question is, how often is ransomware, virus attack or a data breach not a result of weak passwords,[14] a lack of adequate patching, the design of insecure systems by default or just a lack of doing basic daily activities (e.g. monitoring the operations of e.g. your anti-malware software).

9 *Ashenden, "Information Security management: A human challenge?," Information Security Technical Report 13 195-201, United Kingdom, 2008*

10 *B. Lebek, J. Uffen and M. Breitner, "Employees' Information Security Awareness and Behavior; A literature review," in 2013 46th Hawaii International Conference on System Sciences, Hawaii, 2013.*

11 *P. Spurling, "Promoting security awareness and commitment," Information Management & Computer Security, vol. 3, no. 2, pp. 20-26, 1995*

12 *In 2004 Bill Gates had an interview with the BBC where he said, said quote. "E-mail spam will be a thing of the past in two years' time." Source: https://www.businessinsider.com/the-dumbest-things-bill-gates-ever-said-2016-4?international=true&r=US&IR=T*

13 *M. Workman, W. Bommer and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," Computers in Human Behavior, vol. 24, no. 6, p. 2799–2816. And Kabay, "Using Social Psychology to Implement Security Policies," in Computer Security Handbook, 4th Edition , United States, John Wiley & Sons. , 2002.*

14 *In 2018 the most used password was "123456" and on the second "password" Source: https://www.skyhighnetworks.com/cloud-security-blog/skyhigh-research-finds-password-insecure-reuse-cloud/*

Teaser

We believe that the effectiveness of cybersecurity will not increase when more money is added to the IT budget for cybersecurity.

Within business, IT, as well as information security, we often want to go from A to B with a "flashy" roadmap in PowerPoint addressing all the tangible deliverables to get there, which we tend to call "A strategy." The thing is however, if you start researching strategy, you come to the conclusion that it's about more than just a roadmap and the management of that roadmap. Strategy actually has three perspectives:[15] political, economic and technical. The roadmap is the technical part, the economic part is about the funding and the political part is about managing (and influencing) all your internal and external stakeholders to get them moving in the direction you need them to move to achieve a mutual goal. So, when did anyone of us see all these perspectives addressed in an information security strategy document or in the work of security professionals?

Terminology

We started this book with the term information security and Cybersecurity. Digital security is a more comprehensive and overarching term that covers the information security and cybersecurity domain. We use both terms in this book, since they are closely intertwined. Information security was the term used in 1990s and 2000s. Later came cyber-attacks, the dark web, and the deep web, etc., so the term cybersecurity was introduced and became a completely new topic and economy. But what is the difference? Information security refers to actions within a company and cybersecurity is related to external attacks. Nowadays, new perspectives come into play such as:

- Sophistication and dynamics of cyber attacks
- Machine learning and artificial intelligence (algorithms to program machines)
- Virtual identities
- Big Data

15 *Total Competition, Lessons in Strategy from Formula One, Ross Brawn and Adam Parr, 2016*

Teaser

- Distributed hybrid environments (legacy, cloud, Operational Technology (OT))
- New ways of working (DevOps, Agile, Scrum) and autonomy's teams
- Continuous software development (CI/CD)
- Regulatory and assurance (Integrated reporting) (ISAE and SOC2 statements)

With all these actual developments we talk more about digital transformations and safe cloud journeys, so the term digital security is used to cover both domains. In fact, the three terms information security, cybersecurity, and business information security are increasingly being referred to as "*digital security*."

Why this book?

In recent years we as authors have worked in the domain of technology and digital assurance and we have learned the hard way. Helping companies prepare, undergo and recover from all sorts of incidents. In those years we wanted to gain a deeper understanding of root causes and how companies can develop the capability of "antifragility" to cope with stressors and Black swans.[16] We have examined many critical success factors for the implementation and execution of a security strategy.[17] The four main critical factors we have identified are: management and Board commitment, creating a security aware culture, the quality at the top (leadership) and cultivating lessons learned. However, years have passed, and we still don't see any significant change in the way digital security is led, managed, and/or implemented. Still most budgets are spent on technologies, expensive consultants that make PowerPoint presentations, outsourced services, and security products (e.g. insurance). We've seen the same struggle year after year over the last 15 years, apparently without success. Is this because you can't make money on digital security? Is security not sexy enough? Or is it – still – not important enough? Or is the security professional perhaps not capable of demonstrating real business impact or value? In our experience, it's because it takes hard work to change the habits and behavior of people and that

16 *Nassim Taleb wrote in his book Antifragile "When you ask people, 'What's the opposite of fragile?' they tend to say robust, resilient, adaptable, solid, strong. That's not it. The opposite of fragile is something that gains from disorder."*

17 *The book Critical Success Factors for Business Information Security from Bobbert & Papelard (2018) examines top success factors for successful implementation of security.*

is not simply a quick win but requires mental stamina. We also dare to state that in most cases digital security is led, managed, and implemented by people with the wrong skill set.

What will you find in this book?

So, what is this book about? This book describes how to make security a success and turn it into a "cherry experience."[18] We don't want to repeat what others have already written on cybersecurity or things that you already know. So, this book is mostly about the things other security or risk professionals are not talking about, but that are essential for you to know in order to make security a successful discipline in your organization. It will therefore focus more on the strategy, governance, and managerial competences of digital security and less on the technology side. We will not introduce a new control framework or tell you what has already been written by most other authors. We see that the technical side has been described by many people going back centuries. Centuries you ask? Yes centuries. Just think about how old encryption is! No, it was not invented by the Germans in the Second World War; you need to go back to the ancient Egyptians and maybe even further. Cybersecurity from a technology perspective is not new. We called it information security about 20-30 years ago, and before that we had access control and auditor privileges in RACF on mainframes, etc.

The structure of this book

In the following chapters we will write about these non-technical subjects. Often these subjects are actually disciplines from other sciences that we use within the world of cybersecurity. Since we think that the importance of the human factor in security is under-emphasized, this goes for leaders, end-users, IT and other staff responsible for information security measures as well as information security employees, we will therefore largely focus on the people factor. We will not be talking about frameworks because we believe that is akin to focusing on the technocratic

18 *Cherry experience refers to the Dutch expression "Kersensensatie," something that is nice, sweet and has a positive association. The book: "Discover the IT Cherry - How to become the most valued IT organization by using cherries" was written by Mark Butterhoff, Barry Derksen, and Aart van der Vlist.*

Teaser

part of the governance of Infosec. “Technocracy is a proposed system of governance in which decision-makers are selected on the basis of their expertise in a given area of responsibility, particularly with regard to scientific or technical knowledge.”[19] With a technocratic approach, we mean everything that is focused on tools, processes, and certification of the security skills of people, instead of the human factor of leading and changing people and culture to get the security level to the level the company aspires to achieve. Thus, a technocratic approach doesn’t solve the social problems we face in implementing and running digital security. Because we believe the problem is not the latest security tooling or frameworks, the problem is the weakest link ….the human being.

So this book starts with a section on Leading. This section is not only about the leader, e.g. the Chief Information Security Officer (CISO), it’s also about how to lead the company through the cybersecurity challenges and how the CISO role emerges to a Chief Information Security Orchestrator balancing and leading multiple stakeholders. We will not come up with a new organizational design of the security system since we don’t think that this is a key differentiator to make information security a success. A new technocratic organization will not get you to the level where you need to be. Other interventions will, and we will present our key takeaway messages at the end of each section. This way you can read this book as a whole or just read certain sections at a time.

In the second section, we will focus on Strategizing. In digital security the term strategy is often mixed up with plans and the execution of the strategy is lacking. Not because the identified technical improvements aren’t correctly identified, but because the strategy process and content itself is insufficient. Or the people executing the strategy lack the capabilities we have identified. We will address most of these issues and summarize the key takeaway messages at the end of the section.

19 https://en.wikipedia.org/wiki/Technocracy

Teaser

In the third section we will focus on Changing. Changing the people working in digital security and the people who need to act in a secure manner. Because in order to make the human factor stronger, significant changes need to be made. These changes will ideally come from the intrinsic motivation that people want to do well. But why are people resisting this change? Why is it that this current technocratic approach mainly results in more resistance? We will deal with cultural and team change extensively, and of course close with our key takeaway messages.

In the fourth section we will address Governing. We will not design a new governance framework to manage risk, but we will give some tangible practices and metrics to measure and govern your digital security as well as the way to work practically and proactively with your governance, including regulators. Effective governance is about fact-checking, presenting and quantum communicating. Quantum communication means communication needs to be done more intensively (faster, with a higher frequency and more precise) than you have ever done before to keep everyone moving toward the collective destination.

In the fifth section we address the Funding of digital security. As already mentioned, strategy is not only about getting from A to B, but it has also an economic perspective. It has financial consequences that stakeholders want to know about and understand. We urgently need to move away from the Fear, Uncertainty and Doubt (FUD) decision-making and ostrich politics where decision-makers rely on others since "they don't understand it or don't want to understand it." With economic models we bring more rational arguments to the discussion, which enables more balanced decision-making and in the end more "bang for your buck."

In the sixth section we discuss a possible digital security future in Trending, because as a wise man once said: "It's not the strongest of the species that survives, nor the most intelligent that survives. It's the one that is most adaptable to change."[20] (We know, this is a quote that has often been used by other people and that some say that there is insufficient proof that Charles Darwin actually said this.)

20 Quote by Charles Darwin about the evolution of species (some question whether Charles Darwin actually said this)

Teaser

Over the past years of writing, reflecting and getting feedback on our first edition of this book we wrote additional sections that shed new light on the topics we have addressed in that specific chapter of the book. They offer the reader novel insights or new takeaways we did not want to hold back.

To summarize each section, we drafted conclusive “key takeaway messages” to inspire your professional responses. These are quick wins that you can apply immediately or use to initiate meaningful information security conversations within your organization. And, at the end of this book we have formulated, based upon all takeways, twelve final ways about digital security that others don’t talk about, but you definitely should know in order to combat the silent enemy.

Teaser

Teaser

“Management is doing things right; leadership is doing the right things.”

Peter Drucker

01

Teaser

Leading

I told you not to do that…

Digital security within organizations is still seen as a burden and employees still do "stupid things" that they shouldn't be doing, although security staff told them not to do so. The security officers and specialists in organizations usually have a long list of security gaps and actions that need to be resolved and implemented, but still nothing happens, although it seems to be obvious and logical that these issues should be addressed.

We notice that the people responsible for security and "security leadership" often don't sit at the "right table," have limited or no budgets, are pretty much internally focused and the person responsible for security is either a "crack" security expert or has in the opinion of the security staff no idea about security at all. The security team itself is like many teams, a group of individuals who think they're better than everyone else in the team.

Also, security staff are often involved after things have gone wrong. They are often not part of all the fun of creating new stuff, but they are the ones who are expected to clean up and keep firefighting. And how often doesn't it occur that the CIO will ask (or maybe more likely "will tell") the security staff responsible "how could this happen? Why didn't you prevent this from happening?." And, when the security staff are part of new developments, discussions are often about why security measures should be applied and about accepting the risk, instead of being eager to make the information or system as secure as possible.

Of course, the description above is a bit exaggerated. Still, we think most of us would agree that people outside of security don't "really" want to spend their time and budgets on digital security.

Teaser

They want to say A, that security is important and needs to improve, but they don't want to say B, making all the changes and investments to actually be more secure. Also, it's not really nice to work with people who constantly tell you what you're doing wrong and what you should do to be more secure (this also goes for ethical hackers and auditors. Their work is very valuable, but it's the easiest job in security. Identifying vulnerabilities is one thing, but changing an organization toward a more secure one is much more difficult, because people are involved). Although most people currently find digital security important and necessary, they somehow don't want to do anything for it or give away some of the privileges they have. The main question here is, how can we make security everyone's priority and thus lead everyone to a more secure environment?

In our opinion, you need to start with the kind of leadership that guides the company to the right level of security. This requires leadership skills and not just management skills. Second, you need to create the right organization in which the security function can operate efficiently and effectively. Lastly you need the right security team that will take the organization to the next level in digital security, because "if you want to go fast, go alone. If you want to go far, go together."[1]

I have a dream

Leadership has a very long history; some of it goes back to the 6th century B.C. when the Chinese General Sun Tzu wrote "The Art of War." Over the last 180 years we've seen different leadership theories:[2]

- The Great Man Theory (1840 onwards): Thomas Carlyle described the leader as a hero. Although this is an old theory, we still see it used to describe Nelson Mandela, Steve Jobs and Elon Musk.

1 *African proverb that explains that you achieve more when collaborating*

2 *A historical perspective on leadership theories is described in this article. https://leadersquest.org/content/documents/A_short_history_of_leadership_theories.pdf*

Teaser

- Trait Theory (1910-1948): This is about different personality traits and characteristics as the source of great leadership. It's the result of the previous leadership theory, after which investigations started into the nature of effective leadership.
- Behavioral Theory (1950-1970): After research by Stogdill the focus of leadership theory shifted from internal traits to specific behaviors and actions of leaders: are you born as a leader or can leadership be learned?
- Contingency Theory (1967-1990): This is the result of research that showed that no single style of leadership is the right one in all situations. It all depends on e.g. the tasks, situation, the organization, and people involved.
- Leader-Follower Theory (1990 onwards): Leaders assume followers' roles and followers assume leadership roles.[3] The follower is no longer subordinate and obedient of organizational tasks but opens up opportunities for innovation and growth.
- Transformational Leadership Theory (1985-2010): A focus on "transforming" others to get things done instead of mere "transactions." This can be done e.g. by leading by example, offering a compelling vision, using intellectual stimulation.
- Systems Leadership Theory (2015 onwards): This enables the leaders in an organization to create the conditions in which people at all levels can work productively to their full potential.[4] System leadership recognizes that collaboration is essential in solving problems.

So, why do we think leadership is so important for information security?

To explain why we think leadership is so important, let's start with the definition of leadership. Since there is not one universal definition about leadership, here are several definitions:

According to Dwight D. Eisenhower (1890-1969, former president of the United States), leadership is: *The art of getting someone else to do something you want done because he wants to do it.*

3 *Gilbert, Jillian and Matviuk, Sergio (2008) "The Symbiotic Nature of the Leader-Follower relationship and Its Impact on Organizational Effectiveness," Academic Leadership: The Online Journal: Vol. 6 : Iss. 4 , Article 16.*

4 *Systems Leadership, Creating Positive Organisations, Ian McDonald, Catherine Burke, Karl Stewart, 2006*

Teaser

Stephen R Covey defines it as:
"leadership is communicating to another person their worth and potential so clearly they are inspired to see it in themselves."

The army definition of leadership is:
Leadership is the process of influencing people by providing purpose, direction, and motivation to accomplish the mission and improve the organization.[5] *(ADP 6-22, Army leadership)*

According to Warren Bennis,[6] the primary ingredient of leadership is a guiding vision; the leader has a clear idea of what he or she wants to do. The second basic ingredient of leadership is passion. The leader who communicates passion gives hope and inspiration to other people. The last basic ingredient of leadership is integrity.

The essence of these definitions or descriptions of leadership is *to guide people to a certain goal by positively influencing them. Meaning that these people actually* ***wanting*** *to go where they need to go to achieve the goals to be achieved*.

So, when we want an organization to be as secure as we need it to be (the goal), we need to start showing leadership to get there. We need to start influencing the people of the organization positively to make them want a secure organization and everything necessary to get there.

This is not only relevant for the security team, but also for the IT department, HR, Marketing and actually every employee in the organization, and even maybe the customers and suppliers of the organizations since security is only as strong as the weakest link.

So, what does it take to become that good leader? Let's try to find an answer to that question in the next paragraph.

5 *ADP-Army Doctrine Publications 6-22, Army Leadership, August 2012, Headquarters, Department of the Army*
6 *Bennis, Warren. On Becoming a Leader, 2003 revised edition, Basic Books*

Teaser

Do as I say, not as I do?[7]

Defining how to become or be a good leader is not an exact science. Although there are many books on leadership (if you search for leadership on Amazon, you get 70,000 hits), it's hard to have one magic formula for leadership. However, researching the characteristics, or skills that make leaders successful or not, we end up finding some similarities. Below you'll find some models and theories that we came across, that are either really well known by most of us or we believe absolutely valuable to get to understand.

One of the first books ever on leadership is The Art of War by Sun Tzu. Sun Tzu characterized leadership as a mix of five traits: *Intelligence, Credibility, Humaneness, Courage, and Discipline*. As you might have read in some of the leadership theories, the question is whether these are achieved by nature or by nurture.

According to Ron Meyer and Ronald Meijers in their book Leadership Agility,[8] an effective leader *is capable of influencing other people to move in a certain direction*, which can be divided into four elements:

- "***Other people***," which means that it's not about the leader in isolation, but about the interaction between leader and followers, not about what the leader does, but also how the followers react.
- "***Influencing***," which ranges from using formal powers, such as hire, fire, reward, reprimand and reassign, to informal powers such as the ability to convince, charm, inspire, support and challenge. Informal powers are usually more effective and more lasting than formal powers.
- "***Is capable of***" and willing to influence followers. leaders must be willing to take the responsibility of the leadership role and invest in winning authority among potential followers.
- "***To move in a certain direction***" and to realize objectives. It's not the goal to gain powers as an end in itself, but as a means toward achieving objectives.

7 *A quote from the song "Jesus he knows me" by Genesis*

8 *R. Meyer and R. Meijers, Leadership Agility, Developing Your Repertoire of Leadership Styles, 2018*

Teaser

One of the areas that we often refer to in this book is the military. It's interesting to see that in modern free democracies, people still go out to fight a battle that might not be theirs, probably pays little, with the risk of losing everything, namely their life. History teaches us that in war, leadership can make the difference between life and death, between winning and losing a war. The leadership of the army is also fascinating since it has been there for centuries, long before all those leadership books were available on Amazon and before leadership gurus started talking about it in seminars.

An interesting publication of the US Army is the Army Doctrine Publication (ADP) 6-22, "*Army leadership and the profession*." As put forward by the authors in the Introduction:
ADP 6-22 establishes and describes what leaders should be and do. Having a standard set of leader attributes and core leader competencies facilitates focused feedback, education, training, and development across all leadership levels (direct, organizational, and strategic). ADP 6-22 describes enduring concepts of leadership through the core competencies and attributes required of leaders of all cohorts and all organizations, regardless of mission or setting. These principles reflect decades of experience and validated scientific knowledge.

An ideal Army leader serves as a role model through strong intellect, physical presence, professional competence, and moral character. An Army leader is able and willing to act decisively, within superior leaders' intent and purpose, and in the organization's best interests. Army leaders recognize that organizations, built on mutual trust and confidence, accomplish missions.

In the most recent ADP publication (August 2019) a well-defined figure presents a logical map of leadership;[9] however, we believe the overview picture in the 2012 version provides a slightly better overview of leadership.

In addition to the leadership requirements model the 2012 model also stipulates *the levels of leadership and conditions of leadership*. While most of us think of the Army as dictatorial; in which orders are absolute, it refers to *trust, empathy, interpersonal tact, leading by example,*

9 *ADRP 6.22, Army Leadership – August 2019, Headquarters, Department of the Army*

Teaser

Epilog

Cybersecurity has become essential for boards of directors and senior business executives. This shift is driven by regulation, the increasing prominence of cyber-attacks in the global news, or even a cyber incident in their enterprise.

The role of Chief Information Security Officers (CISOs) is evolving towards Digital Security leaders, from being solely technical experts in IT to becoming strategic business enablers and leaders who deliver significant value at the highest levels of corporate governance. As cybersecurity transcends from being exclusively a technical concern to a business value priority, its relevance in boardroom discussions rises significantly. This shift catalyses an enterprise's security program, needing sophisticated execution by the CISO.

Simplicity is critical in security, as complexity poses a significant threat to it. Adopting a straightforward approach in presenting the topic to the board and senior business executives is vital to succeeding as a CISO. I adhere to the 'grandfather test,' ensuring that every message I convey is easily comprehensible, even to someone unfamiliar with security terms. In addition to clear and straightforward communication, an effective security program relies on robust Key Performance Indicators (KPIs) with actionable insights to drive the security agenda enterprise-wide. This is securing funding, appropriate resources, and the right execution from top level governance to the last line of control of an enterprise.

It's also crucial to acknowledge that each organization's security program is unique and shaped by its industry vertical, value chain , and corporate culture. While leveraging globally accepted standards and frameworks (like NIST CSF and ISO27001) is highly recommended, customization to align with the specific needs of the enterprise is essential to foster a business-tuned and value-driven security program in your enterprise.

This book's content helps any digital security leader examine all the relevant perspectives, ranging from governance to funding to measuring value creation. I hope you enjoyed reading and applying it as much as I did. Within ten years, a new edition will emerge in which security is integrated into most of our core activities.

Mathias Bücherl

Group CISO at Heidelberg Materials AG

About the authors

Yuri Bobbert is CEO of Anove International, Global CSO at ON2IT and Academic Director / Professor at Antwerp Management School (AMS). 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 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. In 2021 he published the books "Digital Value creation" and "Strategic Approaches for Security Governance" Bobbert is co-founder of technology solutions such as Anove, SecuriMeter, SECA/Lockchain and Meetingwizard GSS Software. And published 100+ articles.

Mark Butterhoff has gained experience over the last 23 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.

Figures & tables

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) –

"This book effectively dismantles the complexity often associated with Security, offering a holistic, straightforward approach to making it actionable within enterprises. Bridging theoretical models with accessible explanations empowers readers to launch an enterprise security program with ease and comprehension."
– Mathias Bücherl, Group CISO at Heidelberg Materials AG –

"This book is a 'must read' for any manager involved in the topic of digital security."
– Prof. Dr. Ron Meyer –

"A must-read reference guide that connects theories and models to practical instruments and approaches in the field of digital security."
– Prof. Dr. Steven de Haes, Dean at Antwerp Management School –

"When starting in my new CISO role, the book gave me an overview of key topics to consider. It learned me a lot about relevant leadership skills and how to behave in order to become successful as a CISO. By providing insights into relevant research it gives input for decision making and how to approach challenges I encounter."
– Corence Klop, Chief Information Security Officer (CISO) at the Rabobank –

9 789090 335131 >