FOREWORD BY DICK BERLIJN

We live in interesting times. Our world is rapidly changing. Our world is being dominated by opportunities the internet brings us. Whether this concerns intensifying our knowledge, optimizing business processes, applying new technologies, digital trading, our digital environment has brought us numerous opportunities and represents an innovative power that was never experienced in the history of mankind.

This shining medal, however, has a downside. We were naive in bringing new technologies into our world, blinded by the endless opportunities it brings, but vulnerabilities were neither identified as a priority, nor incorporated in an early stage of product development. This has created a society that is very vulnerable to cybercriminals. Abusing data has become a lucrative business, which can have severe disruptive effects. As a consequence, Business Information Security has become a hot topic.

The past ten years, I have had the privilege to work with the cyber experts from Deloitte on increasing awareness of the effects cybercrime can have on our society, both in the public as in the private sector. In these ten years we witnessed a multitude of serious incidents in various organizations, with devastating impact for the parties involved. In some cases it even resulted in bankruptcy of the company.

Before an incident, companies are often sceptical and reluctant in taking appropriate action. It is only after an incident occurs, that they become convinced that something needs to happen and critical measures need to be in place. But thorough analysis of situations, identifying weaknesses and executing improvement plans do not always lead to an improved situation. Because improvement plans are not adequately anchored in the organisation's business discipline, they fail to change an organization's resilience. My experience is that this happens more often than not. The question we need to answer is: "Why should this be so?"

What do these improvement plans lack that make them fail? And what do we need to do to properly anchor Information Security as a Business discipline? In this book Yuri Bobbert and Talitha Papelard describe the critical success factors necessary for implementing effective Business Information Security in an organisation. Read this book!

General (rt.) Dick Berlijn
Former Chief of Defence of the Netherlands

SUMMARY

Friday 12 May 2017: a day to remember or a day to forget? Hospitals, major companies and government offices across the globe were hit by a massive wave of cyber-attacks seizing control of computers until the victims pay a ransom. It is the biggest attack of its kind ever recorded. [1].

People in organizations feel a sense of urgency about information security. The question is no longer *if*, but *when* an organization will fall victim to a cyber-attack. According to Hooper et al [2]. there is greater public emphasis on security, as well as privacy. This has been driven by media reports of e-commerce incidents and data breaches caused by fraud or identity theft. Laws and regulations on data and privacy, such as the General Data Protection Regulation (GDPR) also put pressure on organizations. Social media, too, has opened up a plethora of privacy and security breach possibilities. Against this background of increased opportunity for

information security breaches, and heightened awareness of the repercussions of such breaches, organizations are seeking to protect their information and minimise the risk of possible damage as a result of a breach. Technological disruption and cybersecurity are now top issues in boardrooms across the world. [2] [3]

We observe an increased awareness that adequate Business Information Security (BIS) is needed, but with the increasing complexity of the information security topic, it is important to ask ourselves how we can apply BIS effectively. This requires additional insights into relevant success factors that contribute to existing frameworks and models and also take intangible factors into account. This leads to more effective BIS and enables organisations to gain more control over BIS. This book aims to establish a core set of Critical Success Factors (CSF) that aids organisations in formulating a security strategy or implementing an information security program.

Most critical success factors from our research concern intangible factors. Cultural factors are more effective in improving BIS within organisations than frameworks, rules and procedures. Tangible factors are part of the core set of CSFs (for instance Budget and Comply with law and regulations), but the main conclusion of our research is that intangible factors need to be incorporated into the common frameworks, models and procedure from security communities and bodies.

We started with an extensive literature review to discover what success factors were considered to be successful for effective BIS by academics. The next step was interviewing security experts to find out when they felt most in control of BIS and what factors are crucial for effective BIS. The outcome was a list of 66 critical success factors from a practical and an academic perspective. These factors were funnelled through explorative research methods into a list of the five most critical success factors for effective BIS:

- Senior management commitment all the way up to the board, so that the board has ultimate responsibility for cybersecurity
- Culture; create a culture of acceptance and protection
- The board of directors and senior executives setting the proper tone for the rest of the company
- Lessons learned; having a databreach; never waste a good incident
- Budget; resources and capacity available to set up information security

The CSFs that scored highest on the scale we have established in this research (ranging from 0 to 5) predominantly came from security experts and not from literature research. This is an interesting outcome, that could be explained by the fact that (1) organizations are more influenced by practical input and less by theory and that (2) theoretical frameworks need to be enriched

with practical oriented views and Critical Success Factors. Since we are researchers *and* practitioners – Talitha Director Business Security at Northwave and Yuri interim Chief Information Security Officer at large enterprises – we felt an obligation to review our own findings critically. Therefore we asked contemporary CISO's from large enterprises to reflect on our research findings in the last part of this book.

Hopefully we all learned an important lesson on Friday 12 May and we can learn from this research and the CISO reflections in this book. We have done our best to provide you with new insights into the Critical Success Factors needed to implement an effective Business Information Security Strategy.

PREFACE

Privacy and security are issues we as a society struggle with on a daily basis, both in our private lives and in our work. We all strive to be happy and safety is an important, but also an uncertain factor in our lives. Every week, we see organisations struggling to gain control of information security. When Talitha worked in prison, she felt safer there than she does on the internet these days. In prison there was insight into the threat landscape and the measures to take when threats occur. It was clear and visible. You simply pressed a red button and a guard or fence was there to protect you. The internet, on the other hand, is complex, invisible and difficult to handle. There's a sense of urgency to have information security in place but few know how.

We enjoy our research and work in information security and want to contribute something to the field with this book. We hope to create a better understanding of how to implement information security. We have done this via executing a research

project into Critical Success Factors and substantiate this main research towards CSF's with additional publications in journals and conferences about associated topics (e.g. factors) contributing the success of Business Information Security (BIS). You will find these associated publications printed on azure blue.

With this research-based but business-oriented book we offer a set of core critical success factors that will help organizations gain more control and become less vulnerable, so that they may contribute to a safer internet society.

In the past years we have met many beautiful people who have enriched our life and contributed to the establishment of this book. Special thanks to Hans Mulder, Ad Krikke, Jaya Baloo, Lies Alderlieste, Erik van der Poel for sharing their valuable time and expert knowledge. We have interviewed them a year after our research to reflect on the outcomes. Besides everybody that contributed in this research project we would like to thank our partners Toon Papelard and Nicole Lieberwerth for their continuous support.

It's hard to describe how much energy, knowledge and pleasure these years of research have brought us. It made us wiser and stronger, but also more humble. The longer we worked on this project, the more we realised how little we know and how much there is still to learn. We sincerely hope you will also learn something from our research journey and the practical reflections from contemporary Chief Information Security Officers (CISO's).

Talitha Papelard-Agteres and Yuri Bobbert

1 BACKGROUND

"Information technology has become crucial in the support, sustainability and growth of enterprises. Previously, governing boards and senior management executives could delegate, ignore or avoid IT decisions. In most sectors and industries, such attitudes are now impossible, as enterprises totally rely on IT for their survival and growth" [4]. This increasing dependency on Information technology also leads to the increasing risk of cybercrime. Rapidly evolving security threats pose an ongoing challenge, as companies and governments face an increasingly sophisticated threat environment [5]. Several studies outline the impact on a business if it suffers a security breach. The US National Cybersecurity Alliance found that 60 percent of small companies are unable to sustain their businesses for six months after a cyber-attack. According to the Ponemon Institute, the average cost for small businesses to clean up after a hack is $690,000. For middle market companies, this is estimated at $1 million [6].

At the 2014 world economic forum for the first time two technological risks made it into the evolving risk matrix. In 2017, although only one is included as a current risk ("massive incident of data fraud/theft"), another ("large-scale cyberattacks") came sixth in the list of risks most likely to occur in the next 10 years. [7]

Although information security did not receive adequate attention for years, these days it is at the top of the list of business risks [3]. The question is no longer *if* it will happen, but *when*, and whether the impacted organization has effective information security in place. Overall it appears that many information security programmes are not particularly effective, given numerous recent reports of serious data breaches or business disruptions. Moreover, analysis of discovered breaches suggests that most could have been prevented if the organization had employed ''best practices'' when it comes to information security controls [8].

Understanding the key factors that influence effective BIS is crucial for business leaders; otherwise security problems can occur, which can lead to financial loss, unavailability of critical systems, reputational damage or even bankruptcy [9]. The increasing number of security incidents underscores the need for effective BIS. For effective BIS, more research is needed into the key factors that help businesses to establish and remain control and at the same time add value to the business.

1.1 | What is the problem?

Nowadays companies find it difficult to raise their information security to an appropriate level. The result may be that an organization is unable to make the right choices when making significant investments in BIS, and thus will still not be in control. There is a range of challenges when it comes to effective BIS. We have identified four key problems related to ineffective implementation of information security within organizations. These are described below:

- **Complexity.** Organizations these days are aware that there is a need for BIS [2]. However, because of the complexity of BIS, managers don't know where to start or what is relevant to ensure effective BIS within their organization. Due to the high-profile organizational failures of the past decade, statutory authorities and regulators have created a complex array of new laws and regulations designed to bring about improvements in organizational governance, security, controls and transparency. Previous and new laws on information retention and privacy, coupled with significant threats of information systems disruptions from hackers, worms, viruses and terrorists have resulted in a need for a governance approach to information management, protecting the organization's most critical assets—its information and reputation [10]. The lack of awareness and knowledge of information security [11] fuels

this complexity. This makes it difficult for organizations to determine which factors contribute to the actual improvement of BIS.

- **The absence of intangible factors.** A range of information security models (ISM) and frameworks consisting of policies, procedures, guidelines and activities and associated resources are collectively managed by an organization to protect its information assets. They show the security maturity level of an organization and what action needs to be taken to be in control. But the value of information security depends on more factors than those prescribed in these frameworks and models. Most of these frameworks do not take factors as culture and awareness into account. For example, von Solms et al. describe the fact that frameworks and technology solutions do not guarantee a secure environment for information. Beside these aspects we also need to take the human aspects of information security into consideration [11]. Chang et al. refer to the fact that research into intangible factors, such as management attention, has been limited compared to other, more technical, aspects of security [12].
- **Ineffective security programmes.** According to Steinbart et al. [8] security programmes are not particularly effective, and the result of this is revealed in various reports of incidents, data breaches and business disruptions [13] [14]. While this indicates that many organizations' information security programmes lack effectiveness,

there is little comprehensive research on the necessary or sufficient components for an effective information security programme [8]. What is missing is a clear set of best practices that are needed for an effective security programme.

- **Lack of Information security management and governance**. Von Solms [15] addressed as early as 2009 that Information Security Governance (ISG) is important to have in place in order to improve BIS. According to CSI/FBI Computer Crime and Security Survey [16] economic, financial and risk management aspects of computer security have become more and more important concerns for today's organizations. Such concerns are complement to, rather than substitute for, the technical aspects of computer security. Solid security products or technology alone cannot protect an organization from security breaches. Dhillon et al. [17] explain the importance of structures of responsibility and people integrity in achieving overall security in an organization. Effective information security management and governance seem to be lacking in organizations [18].

As a consequence, there is a clear need to identify critical success factors that can contribute to effective BIS. Over the years much academic attention has been paid to information security. These research efforts did not lead to an increase in information security, let alone a decrease in security inci-

dents. Critical success factors are proposed to add an additional dimension to the current Body of Knowledge (BoK) in order to create more success in practice. However, critical success factors for BIS have not received much attention in the research community. There are related studies about CSFs for Information Technology [19], but research about CSFs related to BIS are rare.

So we arrive at the following problem statement: *"The absence of rigorously examined critical success factors for Business Information Security contributes to ineffective BIS."* The aim of this study is to provide more insight into potential CSFs that can contribute to the BoK and provide organizations with a better instrument that can be used to address the above-mentioned problems.

1.2 | Questions we want to answer

The main objective of this research is to examine CSF from multiple business perspectives that can contribute to developing a framework of critical success factors that will enable organizations to be effective in information security. The main research question to be answered in this research is therefore: *"Which Critical Success Factors – derived from the literature, practitioners and expert opinion – are key for effective Business Information Security?"* To reach the objective of establishing a list with potential critical success factors the following sub-research questions need to be answered:

- *What is considered "successful" with regard to BIS?*
- *Which enablers do we need to have in place as preconditions in order for Business Information Security to succeed?*
- *Which CSFs are relevant for Business Information Security?*
- *Which CSFs are effective for Business Information Security according to the literature and expert views?*

1.3 | The scope of this research project

The scope of this research is to examine CSFs on all organizational levels, regardless of the sector. Whereas Bobbert et al. performed earlier explorative research on Information Security relevant Governance and Executive management practices [20]. Because the context of this research project is the whole organization it takes a different approach. This research, executed in 2016-2017, takes into account that there is increased awareness nowadays of the importance of BIS due to frequent reports on cyberattacks. The concern is more how to make BIS more effective. Because of its similarity, Bobbert & Mulder's research is used as input to examine differences, overlap and possible new insights.

1.4 | The main objective of this research

A paper by Lebek et al. reveals that scientific researchers still tend to focus on quantitative research methods when examining non-quantitative topics, such as awareness and behaviour.

Figure 1 is the result of an extensive literature study that Lebek et al. performed from 2000 to 2012 on 144 publications dealing with employees' security awareness and behaviour. The researchers encourage the application of qualitative and interpretivist studies to explore such deep factors as user misbehaviour and lack of user awareness. There is a need for more qualitative and interpretive studies in the BIS research field, as Workman et al. also found [21]. This is also acknowledged by Dhillon, who states: *"There has been little research in information systems security that can be termed as interpretivist in nature. Generally functionalists do not even acknowledge the existence of such research efforts (ibid.). For them such approaches are 'abstract' and 'too general"* [22]. However, because of increasing dissatisfaction with the prevalent security approaches, there is a growing number of researchers who have begun to consider alternative philosophical viewpoints in their efforts to develop secure information systems.

Another relevant contribution was made by Abraham [24]. She did literature research on publications that examined intangible factors that influence user security behaviour, including the behaviour of senior management and decision-making skills [24]. Her study defined three major themes:

- Management and peer influences
- Deterrence efforts or sanctions
- Rewards and the level of employee participation in security efforts within the organisation.

Management and peer influence relates to the extent to which employees follow guidelines set by management (for instance compliance regulations) through leading by "good example" or setting the "tone at the top." If managers do not act in accordance with their own predefined guidelines, it is likely employees will follow that behaviour [25], causing IS programmes to fail. In her study Abraham noted a lack of studies that empirically evaluate the effects of management's use of security practices on end users' security behaviour.
Deterrence effects or sanctions relates to the effects these measures have on IS behaviour and adoption by employees. Rewarding employees can act as a motivator, creating commitment to IS. This was also found by Spurling in 1995 [26]. *Rewards and the level of employee participation in security efforts in the organisation* relate to the degree of positive influence user participation can have on IS strategy formulation and implementation. If users are involved at an early stage of the IS planning process (i.e. maturing towards a desired state) [26] [27], this contributes to *"improving security control performance through greater awareness, greater alignment between IS security risk management and the business environment, and improved control development"* [28].

Abraham examined 52 studies, studying individuals' IS behaviour. She refers to a lack of qualitative studies that examine group interaction and behaviour using qualitative methods: *"information security is a complex phenomenon and its repercus-*

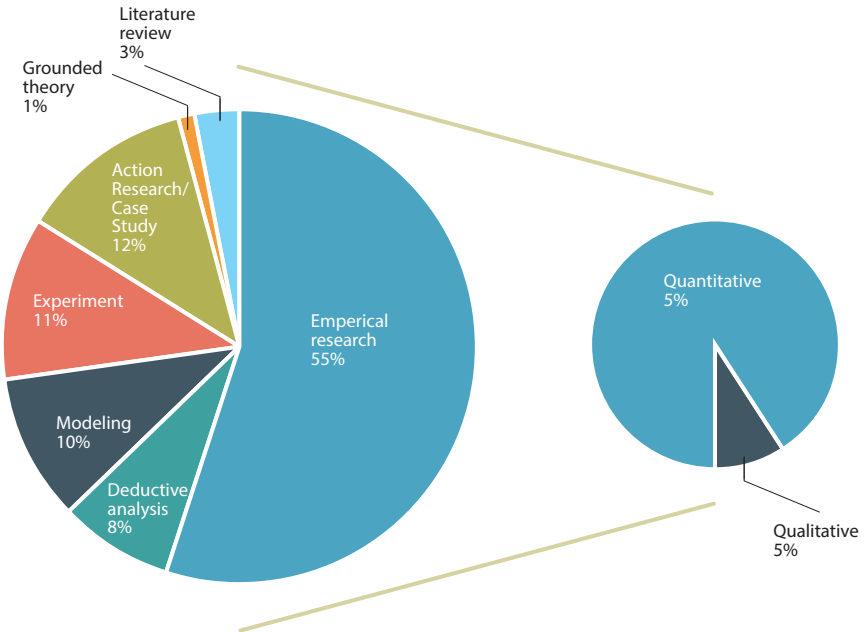

Figure 1: Frequency of applied information security research methods, from Lebek et al. [23].

sions extend beyond individuals to groups and teams in organisations. While numerous studies have addressed end-user security behaviour, we lack studies that examine security group behaviour. Individuals can act differently in group environments especially when groups are responsible for ensuring security. We identify the need for studies that examine the dynamics of security behaviour in group and team settings in organisations." [29] This confirms the importance of qualitative research in this domain.

CRITICAL SUCCESS FACTORS

FOR EFFECTIVE BUSINESS INFORMATION SECURITY

This book describes an extensive research into Critical Success Factors that organisations can adopt in order to improve their CyberSecurity maturity levels. It addresses the concepts of Information Security and CyberSecurity and is substantiated by additional publications the authors have done over the last years. The final set of success factors is reflected via interviews with top Chief Information Security Officers (CISO's) in the Netherlands. This book contributes the academia Body of Knowledge on Information Security as well as providing managers and directors with practical guidance to make their organisation more Cyber resilient.

Talitha Papelard-Agteres MSc is Director Business Security at Northwave. Prior to Northwave Talitha was Manager Security Operations at KPN (Telecom). As researcher at Antwerp Management School Talitha did research in Critical Success Factors for Effective Business Information Security. Talitha is lecturer at several universities in the Netherlands.

Dr. Yuri Bobbert is the global Chief Information Security Officer (CISO) at NN-Group N.V. Yuri is the former CISO of UWV (Government - Financial services) and prior to his role as an interim CISO he served for 10 years as CEO of a consulting firm. He is visiting professor at Antwerp University and is author of several books and publications in Business Information Security Governance and Management.

'*Critical Success Factors for Effective Business Information Security* provides powerful guidance for those looking for practical solutions to the business challenge of cyber risk.'
Dr. Walter W. Bohmayr (Global Head of Cybersecurity Practice The Boston Consulting Group)

DIALOG

9 789461 263117