Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

TC 11 Briefing Papers

# Security of the digital transformation

*Abbas Shahim*

*Vrije Universiteit Amsterdam, Amsterdam, the Netherlands*

ARTICLE INFO

*Article history:*
Received 7 April 2021
Accepted 23 May 2021
Available online 28 May 2021

*Keywords:*
Digital transformation
Digital security
Information security
Digital disruption
IT auditing

ABSTRACT

In the early days of computation the focus was mainly on designing, developing, maintaining, and administering infrastructures and information systems housed in data centers. To this extend, security was traditionally organized around the basic technical components (e.g. data center facilities). The point was that an associated security activity was mostly separated from a business context and in general executed by the technical staff. Security was not fully understood by other audiences because the computer terminologies were frequently used.

When security elements (e.g. logical access protocols used for identification, authentication, authorization) became part of the financial statement audit, its context became clearer, and it was conducted for external auditors. However, the presented outcome of the work was not completely interpretable for these practitioners as again, it was mainly reported in Information Technology (IT) jargon, and was not linked with the financial statement either. With the emergence the Sarbanes–Oxley Act (SOX) and the fundamental role of IT in relation hereto, the context of security suddenly changed to a great extent. The audience extended as compliance, including security, became the dominating item on the agenda of many C-levels (e.g. CFOs).

## 1. Introduction

In the early days of computation the focus was mainly on designing, developing, maintaining, and administering infrastructures and information systems housed in data centers. To this extend, security was traditionally organized around the basic technical components (e.g. data center facilities). The point was that an associated security activity was mostly separated from a business context and in general executed by the technical staff. Security was not fully understood by other audiences because the computer terminologies were frequently used.

When security elements (e.g. logical access protocols used for identification, authentication, authorization) became part of the financial statement audit, its context became clearer, and it was conducted for external auditors. However, the presented outcome of the work was not completely interpretable for these practitioners as again, it was mainly reported in Information Technology (IT) jargon, and was not linked with the financial statement either. With the emergence the Sarbanes–Oxley Act (SOX)[1] and the fundamental role of IT in relation hereto, the context of security suddenly changed to a great

[1] The Sarbanes-Oxley Act of 2002 was developed to emphasis the significance of business control and auditing. It targets to prevent misconduct, improve corporate governance practices and assure the accuracy and completeness of published financial information with the proper administration routines, procedures and control activities.

https://doi.org/10.1016/j.cose.2021.102345

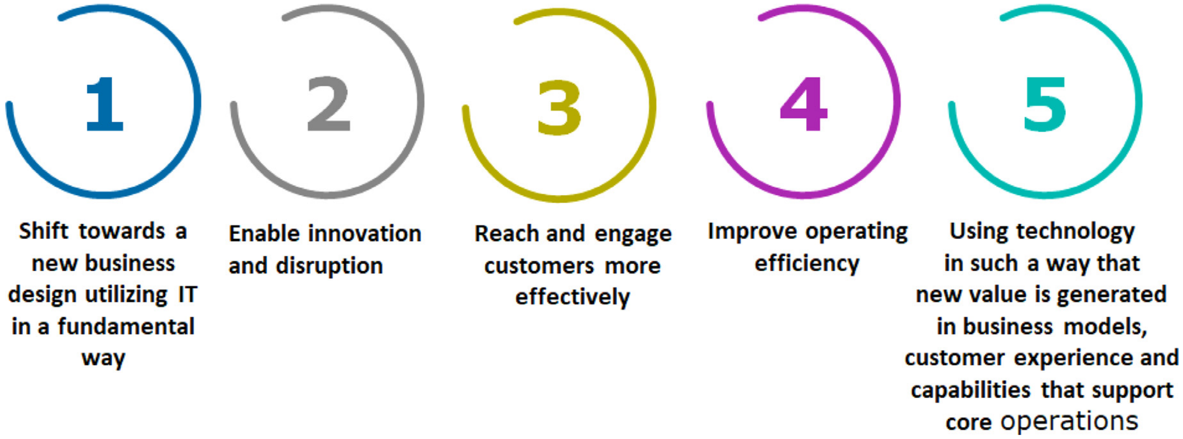
1
Shift towards a new business design utilizing IT in a fundamental way
2
Enable innovation and disruption
3
Reach and engage customers more effectively
4
Improve operating efficiency
5
Using technology in such a way that new value is generated in business models, customer experience and capabilities that support core operations

**Fig. 1 – Aspects of Digital Transformation.**

extent. The audience extended as compliance, including security, became the dominating item on the agenda of many C-levels (e.g. CFOs).

## 2. Digital transformation

Organizations equipped with digitally capable workforces are emerging rapidly, generating value, gaining trust, enlarging the shape of the competitive nature of these days' business, and above all rewriting the industry. As examples, Uber, Alibaba, AirBnB and Picnic[2] are all companies that have disrupted their sector by using technology and have grown to become true IT factories. Picnic has conquered the Dutch market, which represents the highest supermarket density in the world. It is actually not an ordinary and traditional supermarket. In fact, it is a technology company in transition from mobile first strategy to more usage of artificial intelligence that acts as a food logistics company. It places focus on a revolution in the food supply chain through introducing a major change in its sector that causes disruption in business operations (Loohuis, 2017).

Today, there is an interesting dimension added to the way in which organizations deal with clients, and newly satisfy their requirements. It is intensively focused on digitally reaching and attracting the attention of these customers, and involving them at anytime, anywhere and across any device. This revamped world authentically opens the door to an upcoming world in which technology is not only utilized in the back-office, but is fundamentally put at the heart of organizations to transform or replace processes. It has become a core and base part of what they do, enables innovation, assists them to be disruptive perceived as a unique chance to outclass the early adapters and grow, and as such drives their success. This modern approach usually called digital transformation is in general about shifting towards producing business models not existing before, some aspects of which are summarized in Fig. 1.

The aim is to do things in other ways and penetrate new markets to make full use of the growth potential. Applying technology, the digital world and the physical world are fluently integrated to form an attractive one which, by definition, is compelling, leads to fading their boundaries and consequently making them less distinct. This impressive combination presents unparalleled opportunities to seamlessly engage with clients and pleasantly impact their experience. Their needs and wishes for free, intuitive and user-centric products and services are quickly growing, and the fast evolution of technology are lowering the barriers facilitating the entrance of new revenue streams. Digital business generates a US$309B market for technology products and services by 2020 (Gartner 2014; World Economic Forum (WEF) 2016). It is anticipated that the market will grow further reaching US$ 462B by 2024[3]

## 3. Technological embracement

Organizations are taking the chance to gain advantage from continuously evolving technology by leveraging its unique quality and features, and using it as a positive catalyst that helps to realize change. This capitalization truly provides support around the digital transformation ahead of them, powerfully facilitates them to act and behave differently, and reshapes their business in the end. They, among other requirements, need cutting-edge facilities to boost connectivity and conversion, to analyze massive sets of data giving the staff means necessary to empower the digitalization process, and to correspondingly accelerate the intended growth. It has become visible for many organizations what at the minimum the reality of tomorrow is, if not today, which is obviously more than building websites alone. And so, what is hardly required to stay alive and successfully continue operating on the global, competitive, highly demanding, and as-a-service marketplace. In this digital and thriving context, technology is embraced more closely than ever before, is deployed in the way

[2] See www.picnic.nl for further information.

[3] https://www.marketresearchengine.com/digital-transformation-market

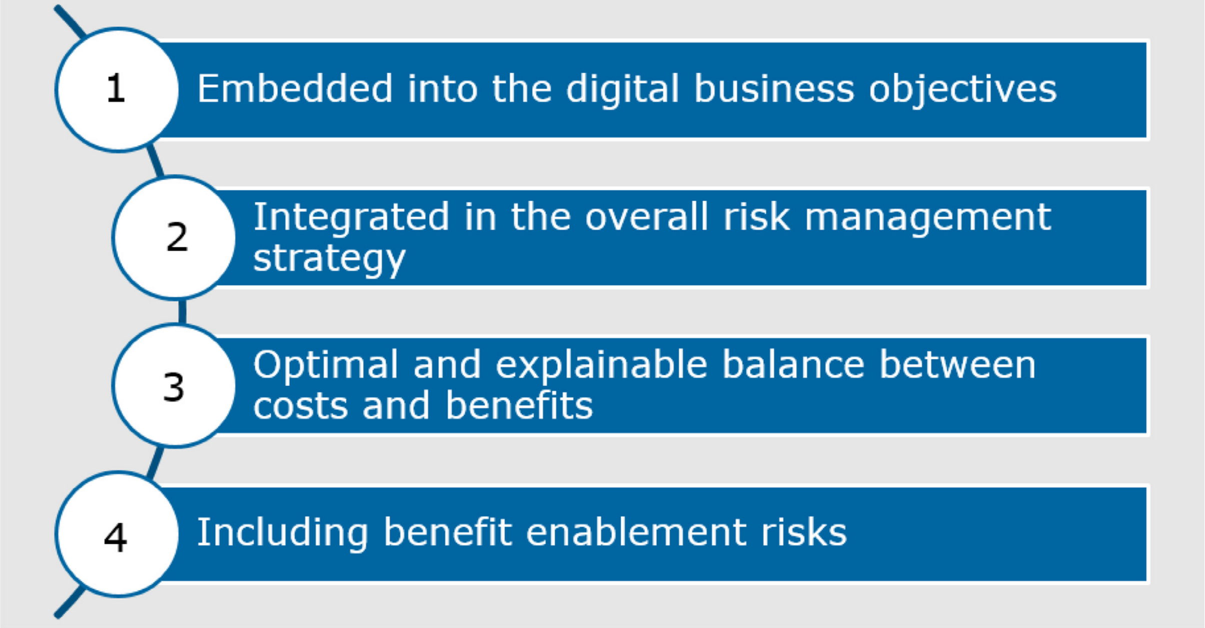
1
Embedded into the digital business objectives
2
Integrated in the overall risk management strategy
3
Optimal and explainable balance between costs and benefits
4
Including benefit enablement risks

**Fig. 2 – Some features of digital security.**

strategies and plans are defined and executed, and influences how new businesses are organized and led.

Therefore, business sectors are increasingly adapting digital enabled business models, and are cognizant of the fact that they should at the very least apply a data-driven approach, employ digital tools and infrastructures to obtain more value, and faithfully play the game by provably adherence to the applicable local and international laws and regulations. Although deployment of a digital landscape offers benefits that are too clear to ignore, it may also expose organizations to severe incidents (e.g. data seen worth stealing by hackers through a targeted attempt) normally due to different levels of access to crucial infrastructures and essential data sources. Risks posed by both insider threats and external cyber attacks impact the business profile as well as the operational model, and must hence be mitigated to appropriately protect the brand and the business assets, and be considered trustworthy at last (Fuze 2016; El Sawy and Pereira, 2013; Applegate et al., 2006).

Issues, concerns and uncertainties with respect to safeguarding the aforementioned aspects are increasing over time. It can be stated that it is now the time for security to derive benefit from the ever-growing and worldwide digital economy. The line of thinking includes a new group of audience other than the well-known roles (e.g. CIO), and embraces a technology-oriented perspective with all its positive as well as negative consequences. This enormous change at global level certainly possesses the potential to pave the road for security to rearrange itself, to create different and maybe even new outcomes, and to refresh its business value.

## 4. Revamping security

Now, there is barely a dividing line to be drawn between business and IT, at least the way in which we historically used to clarify the distinction. IT has already become business. This continuously evolving technology forms the beating heart of organizations, and is thus an essential part of a day-to-day responsibility of average business officials as well as top executives. Their changing view and act for strategizing, steering, transforming, positioning, governing, managing, and running organizations in the digital age calls for a revamped orientation of security. A major key finding of a research among business leaders and Chief Executive Officers (CEOs) with regard to the key business issues facing their organizations was about the new and higher level of security risks created by the digital transformation with which it is not properly dealt yet (Wheeler, 2017). This demanding world characterized by a technology-centric perspective requires a broader and more balanced picture of security. It is important to precisely know the status of the formal and procedural part of security (also referred to by many as security around the IT) put in place. It is also equally important, if not more, to apply an approach towards the hard-core side of security, and with the use of IT. The purpose is to concretely discover the technical security details about the reality of IT, just the way it is without vagueness. In this challenging context, security management is perceived as an instrument that can provide a clear view on the extent to which security is embedded into IT with the aim to ensure that this technology does not affect the risk profile of business practices. In addition, security-thinking as a global discipline can contribute to addressing risks and governance concerns and helps to obtain insight into the achieved degree of trust and acceptance while digitally transforming.

## 5. Positioning digital security

It is obvious nowadays that digital is the foundation of modern organizations and is the key driver and crucial facilitator of their operations. Due to a variety of reasons (including lack of in-depth security knowledge, growing complexity of this ever-evolving topic, misconception of related risks and overhype of specific ones), some substantial risks are often overlooked (e.g. timely patching) or others wrongly get additional attention. Serious failures in digital transformation – be it a service provider that does not meet the security level agreements, an operational crash, a security project that fails to deliver what it sets out to achieve, or a data breach– as a result of misunderstanding of risks related to its application can result in business disruption with undesired or even devastating consequences. At the end of the day, those that are eventually successful in the digital era are those that identify and deal with security risks most efficiently and effectively. Managing them has traditionally been an inescapable part of the daily business and has always formed a concern as such. What is new about this essential topic for many digitally transforming organizations is the appropriate interpretation of business risks in relation to security in a strategic fashion. Digital security risks have already become a business challenge and are no longer merely a technological issue. They are now high impact business risks and should be managed in an interconnected and balanced fashion to create long-term and sustainable gains. It thus calls for an embedded and end-to-end approach convincingly dictating that it is the responsibility of everyone to jointly practice proper security management and prove it to the internal as well as external stakeholders. The demand for security mainly driven by digital transformation could never be greater. But then, this growing need also implies that a new day has come that imposes to technically secure IT and continuously monitor it using IT (i.e. automated tooling) because of the highly ever-increasing level of reliance on technology. This future view on technology-based and technology-enabled security clearly touches the way in which digital transformation is strategized and executed, and generates more value for upcoming digitally-run businesses. In other words, it is now time for security management to reorient and make an impressive impact never experienced before.

## 6. Closing remarks

Security is the cornerstone of the digital transformation and is in the new world all about revamping, strategizing and embedding. This essential topic spans the classic IT security domain, is not restricted to merely protecting infrastructures, and is a pervasive component of the modern business strategy as its related events can negatively influence the intended and desired business outcomes. It therefore aims at specifically mitigating business risks associated with the usage, ownership, operation, impact and adoption of digital technologies. As an ongoing process in any organization and the core part of the daily activities, digital security management possesses several unique features presented in Fig. 2. It is at least embedded into the digital business objectives, is integrated in the overall risk management strategy and is practiced as such, and ensures an optimal and explainable balance between costs and benefits. Unlike the traditional ones with a special focus on IT assets, this established process covers a much broader scope. It also includes benefit enablement risks related to the application of technology to enhance efficiency and effectiveness of the business processes, project risks concerning the contribution of digitalization to new or modernized business solutions, operations and delivery risks connected with the performance of digital platforms, solutions and services supporting daily business operations, and more. This valued undertaking is essential to ensure that security risks are digitally mitigated in such a way that the achievement of digital transformation objectives are not jeopardized.

## Declaration of Competing Interest

This paper is produced by a member of IFIP Technical Committee 11 and has undergone an internal review process amongst 3+ independent reviewers from within the TC.

There are no conflicts of interest.

## REFERENCES

Applegate LM, Austin RD, McFarlan FW. Corporate Information Strategy and Management. McGraw-Hill/Irwin Custom Publishing; 2006.

Bughin J, Chui M, Manyika J. Ten IT-enabled business trends for the decade ahead. McKinsey Q. 2013;13(May).

El Sawy OA, Pereira F. Business Modelling in the Dynamic Digital Space: an Ecosystem Approach. Heidelberg: Springer; 2013.

Fuze. CIO Outlook: Driving Digital Transformation in 2017. Fuze, Inc; 2016.

Loohuis, K.,(2017). Innovatie moet in de organisatie hoogste prioriteit hebben: een interview met Daniel Gebler, Computable, Jaargang 50 | #5 | 2017. (Loohuis, 2017 https://www.computable.nl/artikel/achtergrond/topic-loopbaan/6199199/2978641/picnic-de-moderne-versie-van-de-srv-man.html.

Gartner. Post Event Trip Report: Digital Maturity Benchmark Summary. Gartner, Inc.; 2014.

Moore S. How Board Directors can Remaster Leadership to Win in Digital business: Leadership, Cultural Change and the Right Talent on Your Board are Essential for Digital Transformation. Gartner, Inc.; 2017. August 16 https://www.gartner.com/smarterwithgartner/how-board-directors-can-remaster-leadership-to-win-in-digital-business/ .

World Economic Forum (WEF). Digital Transformation of Industries: Digital Enterprise. World Economic Forum white paper; 2016. January.

Wheeler JA. Top 10 Factors for Integrated Risk Management Success. Gartner, Inc.; 2017. 28 March https://www.gartner.com/en/documents/3645368/top-10-factors-for-integrated-risk-management-success .