Risks and threats in cyberspace – The key to success in digitization

Andrea Strelitz
University of Pannonia Faculty of Business and Economics. Doctoral School of Management Science and Business Administration. Egyetem u. 10. Veszprem H-8200.

Email: streliz.andrea@gmail.com

Abstract. The rapid spread of digitization raises some questions about the sustainability or preparedness of economic associations and their resilience to threats. Based on recently completed research, it can be said, that behind the technology aspect of digitization; it is essential to develop a management approach to reduce the exposure of knowledge stored in data, to threats. Beyond the opportunities provided by digitization, there is a counterweight to the dangers and importance of data protection presented in this study. At the same time, organizations and surveillance systems set up to support data and information protection, as well as cyberattacks, are currently mentioned as some of the most significant risk factors in the world. Then a current research’s results are introduced, on the importance of data protection. Finally, the paper concludes with some cases that have happened in the real world.

1. Introduction
The digitization trend is bringing information technology and automation to a common platform that affects manufacturing-related processes and basic operational functions. The aim is to meet the following four criteria:

1. *Horizontal integration*: The smart factory adapts to the new conditions of its environment and optimizes its production processes, which can be fulfilled in the value chain by integrating customers and suppliers.
2. *Vertical integration*: In a smart factory, people and machines, and resources are mapped in a digital model and communicate with each other through cyber-physical systems (CPS).
3. *Smart products*: They have information about their process. Data is collected and then transmitted to the different production phases.
4. *Human itself*: is at the center as a controller of value creation [1].

In these four criteria, cyber threat is present. The smart factory unit treats the supply chain as an extended operational space for product flow in cyberspace. From this integration, any attack in cyberspace clearly affects the business continuity that exists among parties. In this case, the flow can be interpreted as performance scheduling, money, information, or documents governing collaboration. Where the horizontal extent can be interpreted, the vertical also gives itself. Thus, the cyber threat will act in a vertical direction and affect in a horizontal order, because if a point of integrated operations in cyberspace are damaged from the outside, its impact will affect all participants horizontally.

A smart product is the main purpose of maintaining an integrated operating space in cyberspace, as well as business relationships and continuous business flows (business continuity), but it is also the...
primary target of cyber threats. Thus, the development of the fourth criterion remains at an appropriate level, which is able to make the opportunities provided by digitalisation, in addition to protecting cyberspace, sustainable in the long run and resistant to unexpected threats. At the same time, it must be seen that although a human is able to provide the conditions for safe operation in cyberspace, that is, to create and maintain the first three points of digital transformation, a human is also the one who can attack it and cause serious damage.

Attacks on the digitalisation of business associations are clearly and specifically aimed to be abusive or to gain abusive access. When business flows are impeded, digitized operations immediately lose their value and legitimacy. Thus, in digitization processes, the protection of cyberspace is primarily necessary to maintain business continuity. Under the Sustainability, the simplest overview approach is the solution offered by the International Organization for Standardization, with the ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity standard. This standard is a hybrid solution for ensuring business continuity from the aspect of information technology, ie cyberspace protection. This standard combines the guidelines of two standardized management systems: ISO/IEC 27001: 2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements, which clearly supports information protection, and ISO 22301:2019 Security and Resilience – Business Continuity Management Systems – Requirements, which in turn helps the continuity of business flows from a management aspect. This paper does not aim to detail these standards, but highlights that standardization is a conventional approach that supports the success of the digital transformation in as many ways as possible.

In the IT and banking sectors, business continuity as a term is well known in terms of magnitude, but the same is less true for other industries or sectors, despite the fact that it is not possible to stay out of the digitalisation process and ultimately lose market share. If business continuity, that is, the aspect of business factors, were to be interpreted, Figure 1 helps to illustrate the factors flowing in the business space, which is a mutual cooperation of business participants. From this model, it becomes immediately clear why the IT and banking sectors are at the forefront of business continuity management.

Figure 1. Objects of business flows (Source, Own edit)

Therefore it is easy to see that cybersecurity and business are interdependent, with hand-to-hand operational needs and, in the event of damage, having a crippling effect on the overall flow medium.

Along this line of thought, the issue of cybersecurity will be emphasized in the future, highlighting the dangers of digital transformation, and finally the results of a research will show how cybersecurity, ie the success of digital transformation, is emphasized from a management approach.

To date, the news talks about cyberattacks almost every day [2]. Yet, there is still a majority, who consider themselves untouchable. A cyberattack is never small-scale and never carries a low risk for the
operation of economic agents. Without adequate protection, you can paralyze one or more companies, either temporarily or even permanently. Examined in a network, the injury of a company also affects the operation of its partners. For example, already in 2014, the cost of cybercrime was $ 8.58 in the UK, almost 0.16% of GDP, 0.64% of GDP in the US, and 1.6% in Germany [3], and these amounts are increasing continuously.

According to expert observations and analyses, damage to data and information, or inadequate cybersecurity, has been the world’s most significant risk for years. Some countries are taking this very seriously. Beyond product and process security, a major change in management approach and raising of awareness is needed, to promise a genuinely secure and win-win future for digitized solutions. “...Today, cybersecurity is one of the most important items in the world, more and more people are dealing with it, in an increasingly professional way, but today it is such that I admit that I did it, it doesn’t exist. That’s it, that’s how it works... cyber security has been overrated, but no one has ever recognized it...” [4]

2. The Way to the Concept of Cybersecurity

As the concept of sustainability is already known to all economic participants, in this case, it does not require a more severe and detailed introduction, but its relationship with standards is more interesting.

As a preliminary point, it is worth mentioning that in general, there is not as strong a relationship between data and information protection requirement among industry actors, in the supply chain, as there is for the functional safety of a product. Yet current trends carry the potential for the future when these two preferences are reversed. This is mainly due to the protection of intellectual property, which is the economic operator’s own specific right to exist in the market, and which is the primary property and value to be protected. Recognizing that the safe, functional performance of a product and all business relationships associated with the product are already valuable, in the form of data and information; exposure to this information can clearly and seriously jeopardize even an entire supply chain.

ISO standards and legal obligations for the protection of data and information, as well as hardware, are already available in significant quantities. Instead of a detailed presentation of these regulations and recommendations, it is more important for the standard creators to have a relationship with the Sustainability Efforts, which essentially concludes the Sustainability Aspect of Data and Information Protection [5]. That is, standards should continue to be treated as one of the cornerstones of sustainability efforts; from the point at which the International Organization for Standards has declared its commitment to supporting sustainability, while structuring the standards, concerning sustainability targets and aspirations. Thus, for someone for whom sustainability may be a more distant reason for data and information protection, standards, regulatory recommendations and obligations may be more rational starting points.

Narrowing down this global approach, an effort was launched more than 50 years ago, which has now been defined at a standards level. It has the participation of more than 50 countries and has grown into almost a separate field of science. This is business continuity management; which is about an instruction system, for integrating all currently known disciplines related to management for the future existence and sustainable development of an economic association. One of the milestones in the development of business continuity management, was the promotion of hardware and software for the management, storage, and protection of data and information. Even before the 1970s, the importance of data and information was recognized in business areas, including processes and product levels. All stages of development to date have aimed to avoid loss (and are still defined as the primary goal to date), which can disrupt the functioning of economic operators or, in the worst case, cause its cessation [6].

3. Cyber Risks and Cyber Attacks

The rapid development of digitization and the parallel increase in market competition, by definition, poses ongoing new challenges for data and information protection [7]. The Business Continuity Institute, headquartered in London, but with 43 hubs around the world, several affiliates, and extensive
collaborative relationships with government and international non-governmental organizations; publishes a Horizon Scan Report [8] each year, based on its research, including a global risk assessment, and high-risk events by nation and region. Horizon Scan Reports usually appear at the beginning of the year, with a summary for the previous year and forecasts for the current year. The 2020 Horizon Scan Report established a ranking of 22 potential risks, the first ten elements of which are as follows (unchanged from previous years for the first risk) in Table 1.

Table 1. Ranking of risks to economic operators by 2020 (Source: BCI Horizon Scan Report 2020 [8])

| Ranking | Description                                      | Likelihood | Impact | Risk Index |
|---------|--------------------------------------------------|------------|--------|------------|
| 1       | Cyber-attack & data breach                       | 3.1        | 2.0    | 6.4        |
| 2       | IT and telecom outage                            | 3.0        | 1.8    | 5.4        |
| 3       | Extreme weather events (e.g. floods, storms, freeze, etc.) | 2.9 | 1.7 | 4.9 |
| 4       | Critical infrastructure failure                  | 2.3        | 2.0    | 4.7        |
| 5       | Lack of talent/key skills                       | 2.6        | 1.7    | 4.4        |
| 6       | Regulatory changes                               | 2.6        | 1.7    | 4.4        |
| 7       | Natural disasters (earthquakes, tsunamis, etc.)  | 2.0        | 2.1    | 4.2        |
| 8       | Interruption to utility supply                   | 2.6        | 1.6    | 4.0        |
| 9       | Introduction of new technology (IoT, AI, Big data) | 2.6 | 1.5 | 4.0 |
| 10      | Political change                                 | 2.4        | 1.6    | 3.8        |

The graph below shows the extent to which these risks have a realistic basis (Figure 2) as in the annual increase of cyberattacks. This increase also carries the monetary value of losses faced by those affected. The number of cyberattacks increased by 600% during the period of Covid19, which was completed by 2020 [9].

Figure 2. Ranking of risks for economic operators by 2020 (Source: PurpleSec [9])

In addition to the annual Horizon Scan Report, the Ponemon Institute, Varonis Data Lab, Veritis Transcend, Cyber Observer, and other organizations are constantly monitoring the evolution of digitization and the concomitant increase in the exposure to cyberattacks. These organizations conduct investigations, analyze cyberattacks and continuously publish vulnerabilities in hardware and software; which serve as warning signals to economic operators, as potential risks to protect themselves, their
products, and their development. Although these reports sometimes show different data, there are no differences in magnitude. Furthermore, there are more than 10 real-time cyberattack monitoring systems available. Kaspersky [10] shows Planet Earth, the flow of attacks, and statistics can be read next to it. Finally, it is worth noting that there is a 100-point, globally interpretable, unified protection strategy, to support data and information security systems [11].

3.1. Personal Experience

Finally, the potential dangers of digitization without an emphasis on cybersecurity are worth mentioning, based solely on personal experience in Hungary. In the examples below, in terms of industry involvement, there are two automotive suppliers.

- **2017**: Large company. Mail received by email. Paralysis of the entire server froze business, manufacturing, and other operational processes. Some data, documents, contracts, others have disappeared from the server. Delivery and manufacturing disruptions. It has become an international investigation; the perpetrator has yet to be found.
- **2018**: SME company. The employee had correspondence related to the payment of an invoice. She approved and installed a new bank account number without any kind of verification. Finally she approved the payment. Following the supplier’s letter of formal notice, it emerged that an alternative “3rd party” had communicated with this employee, without any knowledge of the contracted partners. Serious loss of money. It has become an international investigation; the perpetrator is still out there.
- **2020**: SME company. Also, an email attack. Operational documentation, product documentation, contracts, and more have disappeared. The company was unable to prepare for an upcoming ISO audit, because the entire management system (at the documentation level) was also lost. There is no information on the outcome of the investigation or the audit.

It is to see, in ordinary language, a person turns around and is facing step by step a cyberattack incident in Hungary. The losses of the companies concerned, are most pronounced in the continuity of operations, or in other words, in the course of business, as well as in recovery, in terms of money, production of products, or provision of services and in time.

4. Some Relevant Research Findings

In this section, the initial state that determines the success of digitization in Hungary is presented. The following introduced results are from finished research. It is necessary to add to the results that the main goal of the research is not the answers sought in connection with the development of digitalization, but it has become clear that the issue of information security, ie the realization of a successful digital transformation, emerges only in terms of business continuity.

The main aim of the research was to explore the conditions and factors for business continuity; the sustainability and resilience of an economic association to threats. That is, the research sought to answer the question of what factors, with its harmonious management, a company can survive in the long run depending on the current development trends.

As a result of text analysis from the international literature, 19 key factors as possible business impacts have been identified, which reflect well the global development direction. This result presents that the operation of an economic association can no longer be influenced, and performance cannot be characterized by a single indicator. Complex areas of management and disciplines have emerged that practically point to an integrated, holistic approach, or in other words; the time of one- and two-step linear thinking is over. As a result of the research, the fact was confirmed that an economic association is a complex multidimensional space, which is stretched by market space and time dimensions as well. The 19 potential business impacts (Table 2), the combined and harmonious operation of which will result in a sustainable and constantly evolving economic association, are as follows:
Table 2. Impacts on business in the 21st century (Source: Own research results)

| Topic          | Label               | Coherence | Prevalence |
|----------------|---------------------|-----------|------------|
| t1             | business_continuity| 0.13735   | 6.21549    |
| t2             | human_resource     | 0.02246   | 5.66995    |
| t3             | business_network   | 0.06047   | 3.81966    |
| t4             | business_risk      | 0.07635   | 4.23966    |
| t5             | business_model     | 0.10652   | 5.04932    |
| t6             | organizational_culture | 0.02459 | 5.07255    |
| t7             | enterprise_risk    | 0.02989   | 5.64945    |
| t8             | market_positioning | 0.12587   | 4.52991    |
| t9             | big_data           | 0.02370   | 3.90830    |
| t10            | social_media       | 0.04686   | 5.02789    |
| t11            | risk_management    | 0.08354   | 5.44366    |
| t12            | intellectual_capital | 0.03638  | 8.02514    |
| t13            | international_business | 0.01103 | 4.91318    |
| t14            | core_competence    | 0.02293   | 9.31122    |
| t15            | business_education | 0.08628   | 4.90150    |
| t16            | renewable_energy   | 0.07543   | 5.44473    |
| t17            | risk_factors       | 0.00889   | 3.79179    |
| t18            | business_aptness   | 0.08580   | 4.13105    |
| t19            | supply_chain       | 0.11230   | 4.85555    |

The Prevalence values, essentially return a ranking of values, that can be interpreted as the hottest topics among international publications. From this, it can be concluded that a long-term future perspective is expected for those economic associations, that emphasize (highlighting only the top 3) the importance of “core competence”, “intellectual capital”, and “business continuity”. This ranking of values also indicates that the biggest challenge in this line is in the life of economic associations. It can also be seen that “big data”, “risk management”, and “social media” factors, relevant to digitization, are dealt with on average in the international literature. However, this amount is not negligible either, as text analysis algorithms have highlighted it. The impact on the 19 business impacts, can be characterized by four pillars, with interpreted and integrated narrowing; which means they give the stability and resilience to the unexpected threat and the long-term perspective. These pillars are interdependent:

- **risks** (business, IT, other),
- **networks** (data and information, supply chain, business relations, other),
- **human factors** (knowledge, health, culture, communication, other),
- **management elements** (strategy, market, other) would be the main focus of scientists.

The business impacts are together, a visible summary on the international level, of collective consciousness, from which, depending on the fit, the maturity and values of different countries, sustainability, and resistance to threats can be determined. Examining this set, the difference among large companies operating in Hungary (Table 3) is important.

The effects for which Hungary is strongly relevant to international relevance, have been marked in green. Blue and red marked business impacts are those factors that tend to fit in the rather strong and less strong majority, in line with international expert opinion. In the case of uncolored lines, it can be said that Hungary differs from international trends.

Thus, the economic associations operating in Hungary are strong in 5-8 factors – which can also be interpreted as a management system – and are in line with international guidelines. However, the point is more in the unmarked factors; on the one hand, as in the maximum of 8, is less than half of the total stock compared to 19, and among them are “big data”, “risk management” and “social media”, which
together focus specifically on data management, data protection, and defense and awareness against cyber-attacks.

Table 3. The fit of the effects of the international space on business in Hungary (Source: Own research result)

| Topic       | Label               | Coherence | Prevalence |
|-------------|---------------------|-----------|------------|
| t1          | business_continuity | 0.13735   | 6.21549    |
| t2          | human_resource      | 0.02246   | 5.66995    |
| t3          | business_network    | 0.06047   | 3.81966    |
| t4          | business_risk       | 0.07635   | 4.23966    |
| t5          | business_model      | 0.10652   | 5.04932    |
| t6          | organizational_culture | 0.02459 | 5.07255    |
| t7          | enterprise_risk     | 0.02989   | 5.64945    |
| t8          | market_positioning  | 0.12587   | 4.52991    |
| t9          | big_data            | 0.02370   | 3.90830    |
| t10         | social_media        | 0.04686   | 5.02789    |
| t11         | risk_management     | 0.08354   | 5.44366    |
| t12         | intellectual_capital| 0.03638   | 8.02514    |
| t13         | international_business | 0.01103 | 4.91318    |
| t14         | core_competence     | 0.02293   | 9.31122    |
| t15         | business_education  | 0.06828   | 4.90150    |
| t16         | renewable_energy    | 0.07543   | 5.44473    |
| t17         | risk_factors        | 0.00889   | 3.79179    |
| t18         | business_aptness    | 0.08580   | 4.13105    |
| t19         | supply_chain        | 0.11230   | 4.85555    |

Examining these Business impacts in more detail, comparing them with the integration of companies operating in Hungary; raises some questions about awareness and an integrated approach. For example, how do risks separate, like “risk management”, from “business risk”? Why do company leaders interpret these two related factors separately? This phenomenon can be explained by the fact that 73% of the participants in the study are Hungarian-owned and typically more than 10-year-old companies. That is, the responding business leaders who grew along, did with the values of a different era; operating their companies along with other focus issues and factors. At the same time, it also means the message, that risk management as a protective mindset and management tool, has not been homogeneously integrated into the corporate public consciousness operating in Hungary. The other striking phenomenon is that although human resources as a field of science and management tool has a significant history in Hungary, the respondents do not treat it with a set of knowledge factors. This articulated approach is a kind of message, that human resource management, as the most widely interpreted field of science, is separated during its practical application. That means this field as well, has not yet been fully integrated into the corporate public consciousness, operating in Hungary. As this table is based on the answers to the questions on success and maturity, trends can be identified for all non-colored factors. In the case of areas that can be interpreted in a set at the scientific level; the strengthening of integrated thinking can also be interpreted as a way of development. The table also shows a strong business-centric approach in the focus of companies operating in Hungary, which may be the reason for their survival so far; together with any exposure that differs from the opinion of the international professional community. However, research suggests that leaders of this articulated mindset, perceive their weaknesses relative to the international scientist space and are open to new approaches and attitudes. Referring back to the four criteria, an integrated approach and development of “risk management” and “human resource” management are essential for successful digitization.
5. Summary

Thus, a characteristic of the Hungarian management approach is in implying integrability, covering any segment of the digital transformation and the points at which expected difficulties can be anticipated. If there is a lag in Hungary in the areas of management, raised by the examined ten years of international literature, then this disadvantage is the point from which digitization and its integration into general operation can start.

Digitization is nothing else than transferring certain parts of knowledge and operations to cyberspace and the exploitation of additional competitive advantages in it. The language of digitization is data and information, the flow, access, use, searchability, or protection, which must be given drastic emphasis for successful digital transformation. The general effort in this direction in Hungary is clear, typically supported by strategy [1]. However, the research results suggest that the potential retaliatory threats associated with the means of digitization, data, and information are not yet adequately addressed or in consciousness.

Digitization as a way of development is unstoppable, but the first stable point becomes visible when the knowledge and operation in cyberspace are protected from all kinds of threats, secure, and thus there are no or moderate crippling retrospective risks.

The main conclusions of the research can be summarized as follows:
- Fulfillment of the four criteria clearly and emphatically affects automotive players.
- With regard to the relocation of the relevant operations of the automotive industry to cyberspace, exposure to cyber threats is high, due to the size of supply chains.
- It is essential to increase the cybersecurity awareness of automotive partners operating in Hungary.
- Risk management and human resource management, as essential components of cybersecurity, require strong integration and higher awareness, for successful digitization processes for the future.

Overall, digitization efforts are encouraging, with the resulting competitive advantages, so it is worth emphasizing protection against cyberattacks.

Acknowledgments

I would like to thank Dr. László Berényi for his support in presenting the research results presented in this paper.

References

[1] Katona A, Göllény-Kovács N, Péter E 2020 Az Ipar 4.0 vizsgálata a stratégia és szervezet, munkavállalók és új digitális technológiák oldaláról. XXVI. Ifjúsági Tudományos Fórum, 2020. május 21. Keszthely

[2] Cohen Z, Fung B, Sands G, Marquardt A 2020 US cybersecurity agency warns suspected Russian hacking campaign broader than previously believed. CNN. 2020. december 18.

[3] Chaabouni M 2016 Importance of Business Continuity in today’s business Management – Socio cultural study & expert recommendations. EPFL 2008 – MBA Hult 2015. Available at: https://www.academia.edu/24953112/Importance_of_Business_Continuity_in_todays_business_Management_Socio_cultural_study_and_expert_recommendations [Accessed: 12.01.2021]

[4] Nógrádi Gy 2017 A világ Trump után. Előadás – Budakeszi, Erkel Ferenc Művelődési Központ 2017.06.07. 19:00. Available at: https://www.youtube.com/watch?v=P1-uaXKefRg [Accessed: 13.01.2021]

[5] International Organization for Standards n/a. Available at: https://www.iso.org/standards.html [Accessed: 13.01.2021]

[6] Strelicz A 2017 A gazdálkodó szervezet fenntartható fejlődését támogató kiegészítő irányítási rendszerek (ISO 22301 Üzletmenet folytonosság irányítási rendszer). Nemzetközi Karbantartási Konferencia. ISBN 978-963-396-099-8
[7] Veritis 2019 Disaster Recovery 2019 Statistics – Insights That Shape Your Business Future. 23rd Jun 2019. Available at: www.veritis.com/blog/disaster-recovery-2019-statistics-insights-that-shape-your-business-future/lished

[8] BCI 2020 BCI Horizon Scan Report 2020: An examination of the risk landscape for resilience professionals. Available at: https://www.bsigroup.com/localfiles/en-gb/iso-22301/resources/bci-horizon-scan-report-2020.pdf Figure 3. Risk and Threat Index: Next 12 Months [Accessed: 13.01.2021].

[9] PurpleSec LLC 2020 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. Available at: https://purplesec.us/resources/cyber-security-statistics/ [Accessed: 28.12.2020]

[10] Kaspersky Available at: https://cybermap.kaspersky.com/de [Accessed: 14.01.2021]

[11] Blokdijk G 2008 Disaster Recovery 100 Success Secrets: IT Business Continuity, Disaster Recovery Planning and Services. Emereo Pty Limited. ISBN: 978-0980471663