BUSINESS STRATEGY ANALYSIS OF CYBERSECURITY INCIDENTS

Zsolt BEDERNA
Óbuda University, Budapest, Hungary
bederna.zsolt@stud.uni-obuda.hu

Zoltan RAJNAI
Óbuda University, Budapest, Hungary
rajnai.zoltan@bgk.uni-obuda.hu

Tamas SZADECZKY
Masaryk University, Brno, Czech Republic
szadeczky.tamas@gtk.bme.hu

ABSTRACT

In the current social and economic processes, information and communication services play a decisive role, changing several entities' operations. The growing dependence that has developed over the last two decades made the security needs introduced political will, which has resulted in an iterative evolution of the regulatory environment. Hence, the legal framework requires that several entities develop protection that includes controls enhancing both preventive and reactive in a risk-proportionate manner under the business value to be protected. Nevertheless, due to the nature of cybersecurity, the development of such capabilities is not the task of a single organisation but all entities involved in cyberspace, including, e.g., individuals, non-profit and for-profit organisations, public sector actors. Therefore, each involved entity should design protection capabilities in a risk-proportionate manner, which requires strategic approaches and tools and requires organisations to learn from security incidents. This paper reviews the essential formal security strategy formulation tools, applying in the Facebook's case based on publicly available information. The analysis aims to confirm the importance of management's attitude and support for tackling cybersecurity's challenges.

KEYWORDS: cybersecurity, cybersecurity capabilities, cybersecurity strategy

1. Introduction

As a result of the dynamic development of technology, the information society is increasingly dependent on information and communication technologies (ICTs). Due to its widely applied nature, the commission of crimes has also extended to cyberspace, which world ICTs create. As applied by the European Union (European Commission, 2012), cybercrime is a crime committed using or against electronic communications networks and information systems. This approach comprises the dual nature of cybercrimes as their impacts may be limited to cyberspace or, where appropriate, they may also affect physical space.

However, at first, it is necessary to identify the stakeholders of cyberspace operations. The approach and the mathematical apparatus that the game

DOI: 10.2478/raft-2021-0020

theory of Neumann and Morgenstern (von Neumann & Morgenstern, 2007) defines is suitable for the analysis of both cyberspace operations (Alpcan & Başar, 2010) and data protection activities (Manshaei, Zhu, Alpcan, Basar, & Hubaux, 2013). In general, a security game is determined by the players and the possible steps (actions and reactions) for the players, the pay-off and cost of steps, and the limited information and resources available. There are two different types of players with opposite goals (Emmanuel Chukwudi, 2017): the system's defender and the attacker. Without debt, the purpose of the defending entities is to properly design and operate IT services that support the business missions, objectives, and goals.

Nevertheless, according to the balanced operational constraints, security controls that hinder or even prevent achieving business goals are not acceptable (Wheeler, 2011). However, several defender entities do not tackle cybersecurity with the required priority. For example, managers may view cybersecurity as an unnecessary functionality that the legislation requires somehow due to inadequate knowledge or negative attitude. The results of a survey conducted by Ernst & Young between August and October 2019 (Ernst & Young, 2020) supports the existence of this issue, in which the respondents (N ≈ 1300) were information security managers or had equivalent position. Only 36 per cent of respondents said that cybersecurity was part of the process from the beginning in the organisation they represent.

Howsoever, despite the exact objectives, incidents occur from time to time – some of them consciously according to risk proportionality and some of them unwillingly. Therefore, incident management can lead to unforeseen additional resource expenditure and, thus, additional expenditure regarding the nature and extent of business processes' involvement. For this reason, one may raise the questions of what effects the incidents have and how the entities feed the conclusions drawn back into the strategy, including public entities responding to current challenges (Dawson, Bacius, Gouveia, & Vassilakos, 2021).

To answer these questions, Section 4 discusses incidents affecting Facebook's services. Based on the reviews, in Section 5, a SWOT analysis show the strengths, weaknesses, opportunities, and threats of the given entity, helping to understand the strategies they chose. Helping the analysis, Section 2 defines the frame of the SWOT analysis and respectively, Section 3 discusses strategy formulation. Finally, the paper closes the conclusion in Section 6.

2. Capability Analysis

In the case of defensive entities, to achieve the set of goals according to the defined mission and objectives, planning and strategy creation are essential for an entity's proper functioning. So, it is required to clarify the current operational capabilities and circumstances, for which SWOT analysis is one of the essential tools.

In SWOT analysis, one examines internal and external factors. Internal factors are the parameters that an entity may influence, in which Strengths and Weaknesses are distinguished. On the other hand, an entity cannot directly influence the external factor. This group includes Opportunities and Threats.

Defenders shall determine cybersecurity goals, strategy, the portfolio that implements the strategy, and design security controls in an integrated fashion based on business goals. Therefore, cybersecurity strategy corresponds to the high-level declaration of intent, which, depending on leadership skills, may provide strength or, conversely, weakness regarding their appropriateness. The external factor pair of cybersecurity strategy arises from the organisation's surroundings, which comprise the political environment and national goals and values. For example, the European Union has

begun to develop its cyber defence capabilities based on the Digital Single Market relying on Union-level, Member State level, and organisational entities.

However, the amount that a defendant can spend on supporting the strategy implementation with the establishment and maintenance of security controls relies on the extent of the available financial resources. As entities do not operate in silos, fiscal circumstances belong to internal and external factors due to the dynamic and interconnected environment.

Howsoever, the administrative, physical, and logical security controls must be well-designed and maintained according to the principles of defence in depth and diversity of defence, and the concept of principles of Least privilege and Separation of Duties. On the other hand, the appropriate combination of the deterrent, preventive, corrective, recovery, detective, and compensating controls should be used to manage the risks complying with internal standards. These controls serve the confidentiality, integrity and availability of the data stored in the systems. Hence, depending on its quality, this control mix can be a strength or even a weakness.

However, external influencing factors also arise from legislation and international and industry standards. For example, the legislation defining the cybersecurity policy objectives in the European Union comprises the NIS Directive (Directive (EU) 2016 / 1148, 2016), the GDPR (Regulation (EU) 2016 / 679, 2016), the eIDAS Regulation (Regulation (EU) No 910 / 2014, 2014) and the PSD2 Directive (Directive (EU) 2015 / 2366, 2015) and its implementation by the Member States. ISO / IEC 27001:2013 (ISO / IEC, 2013) and the PCI-DSS (Payment Card Industry Data Security Standard) (PCI Security Standards Council, 2018) are examples of the basic standard for information security.

Nevertheless, relevant laws and standards may push the progress and advancement of security. However, on the other hand, confusion, contradiction, and additional expenses may arise as negative impacts, for example, in the form of a penalty. As the evidence of increasing complexity, there may be an obligation for a defender entity in the European Union to notify and cooperate with different competent authorities in the event of a cybersecurity incident according to (1) Articles 6, 14 and 16 of the NIS Directive, (2) Articles 33 and 34 of the GDPR, (3) Article 19 of eIDAS, and (4) Article 19 of PSD2.

3. Formulation of Strategy

The planning of the security strategy is an unavoidable part of an information, IT, or cybersecurity management system, which has to reflect the reaching of the external and the internal requirements set of the given organisation. According to Alfred D Chandler (Chandler, 1962), a corporate strategy is defining long-term goals, the allocation of resources, and the directions of action to achieve the goals. In a general sense, the strategy answers how management sets goals and supervises managers to achieve them.

The Balanced Scorecard (BSC) framework (Kaplan & Norton, 1992) of Kaplan and Norton is a crucial tool in developing and monitoring the implementation of the strategy via the defined indicators, regardless of the applied strategic management theory (Omalaja, Eruola, & College, 2011). The BSC guides the strategy's development through the Financial Perspective, the Customer Perspective, Internal Business Processes and Learning and Growth (Figure no. 1).

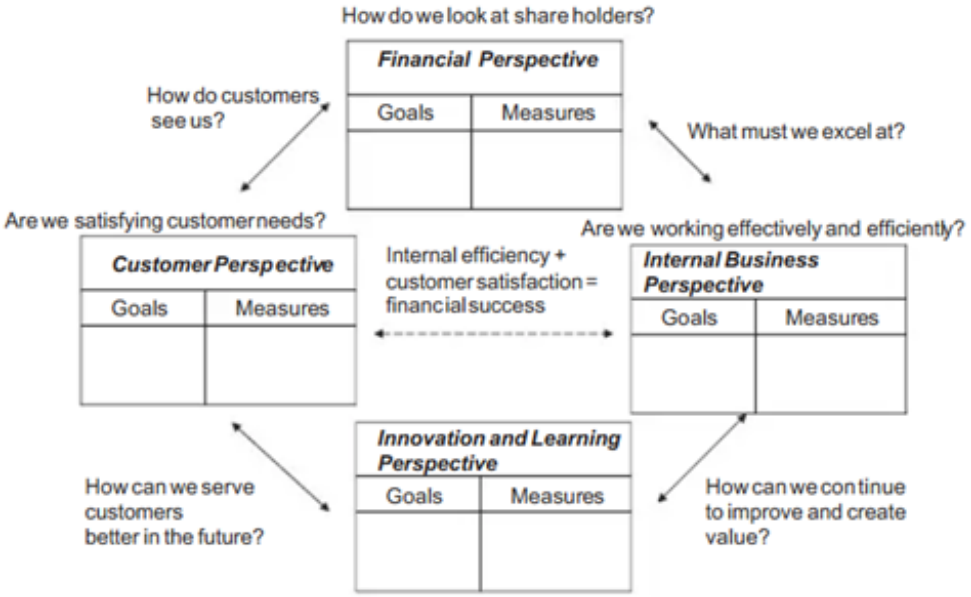

Figure no. 1: *Balanced Scorecard*
(Source: Kaplan & Norton, 1992)

The BSC has undergone several iterative developments since its first release. Part of the framework's development was its extension to other fields as IT BSC and IT and cybersecurity BSC.

The IT BSC (Van Grembergen, 2000) is in the analogy of the original structure through User orientation, Business contribution, Operational excellence, and Future orientation lead by the business strategy. The User Orientation perspective represents the IT user assessment, and the Operational Excellence perspective comprises the IT processes used to develop and deliver applications. The Future Orientation covers the human and technological resources needed to provide IT and services, while the Business Contribution perspective captures IT investments' business value.

Unsurprisingly, the security BSC (Herath, Herath, & Bremser, 2010) is in parallel with the IT BSC. The security BSCs have the Business Value perspective, the Stakeholder Orientation perspective, the Internal Processes perspective, and the Future Readiness perspective. Business value is provided by ensuring confidentiality, availability, integrity, and authenticity and non-repudiation. Stakeholder consideration reflects the needs of the roles associated with a given service. Internal Processes cover the cost-effective design, development, oversight and maintenance of controls based on business objectives using risk analysis. Future Preparedness helps prepare proactively for unexpected situations and emerging threats through staff and users' continuous training.

4. Case Study

In the case of Facebook, the most widely known incident happened in 2014, when Cambridge Analytica collected Facebook user profiles in both unethical and non-legal ways. The first information was that the number of affected users is about 50 million users (The Guardian, 2018). However, subsequent reports indicated that only the number of affected users by the data leak in the United States is about 87 million (Business Insider, 2019). The Guardian first reported the incident in December 2015 (The Guardian, 2015); then more information appeared in The New York Times in November 2016 (The New York Times, 2016), Das Magazin in December 2016 (Das Magazin, 2016), The Guardian (The Guardian, 2017) and

The Intercept (The Intercept, 2017) in March 2017 .

Subsequently, on 28 September 2018, the company announced that, due to data theft, attackers had compromised user data by exploiting a logical vulnerability. Criminals stole the personal information of about 29 million Facebook users, such as date of birth, phone number, search history, and last login location. Besides, the attacker gained access to user access tokens, giving them a chance to access the Facebook accounts of the affected users and other services (e.g., Tinder, Spotify, Airbnb) for which the user had registered their Facebook account (Business Insider, 2018).

In the middle of March 2019, the bad news was the departure of product manager Chris Cox and vice president Chris Daniels of WhatsApp and the Needham downgrade. However, on 13 March, several hours of service outages affected all services due to an application error (The Verge, 2019).

On 24 March 2019, Facebook reported a security incident involving the Instagram service that the company detected during a routine security check back in January (Facebook, 2019), in which internal staff could access masked passwords of Instagram users. Facebook published an updated notification on 18 April 2019 stating that passwords were also stored in an unencrypted manner.

On 12 June 2019, after the leakage of the letter from CEO Mark Zuckerberg concerning potentially problematic privacy practices, Facebook shares fell 2.9 per cent (Markets Insider, 2019). However, despite the fines and additional security incidents (e.g., in September 2019, Techcrunch reported data leaks due to several unencrypted databases with 419 million records (Techcrunch, 2019), Facebook's Q3 2019 results exceeded the analysts' and the investors' expectations (CNBC, 2019).

5. SWOT and Strategy Analysis

The decline of the market share of the Facebook platform begun in March 2017 (Figure no. 2). This trend's catalyst is one of the consequences of the loss of confidence due to the Cambridge Analytica incident's impact. Although this trend did not jeopardise the market leader position, the market loss did impact revenues.

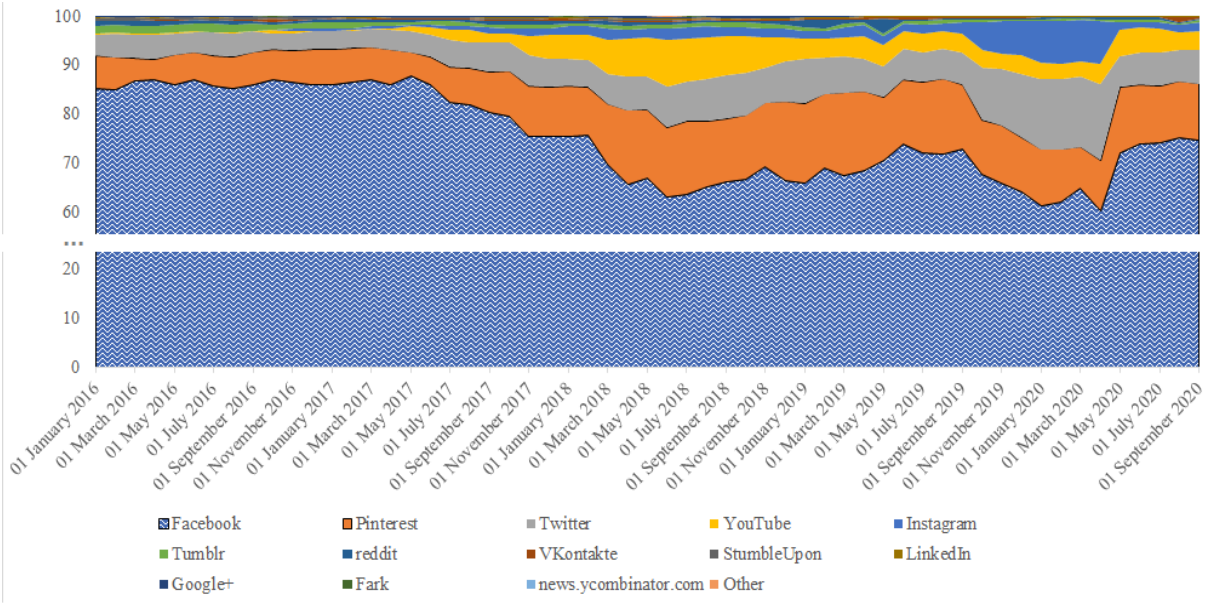

Figure no. 2: Market share of social media services (January 2016 – September 2020)
(Source: Author edits using, Star Counter, 2020)

Regarding the discussion and, the following figure (Figure no. 3) highlights Facebook's internal capabilities and external factors:

Figure no. 3: SWOT analysis – Facebook (2019)
(Source: Author)

Reviewing the information available on the Facebook webpage (Facebook, 2020), the company's mission and corporate values and security values were defined as follows (Figure no. 4) according to the BSC. However, there was no information about concrete strategic elements for all BSC perspectives.

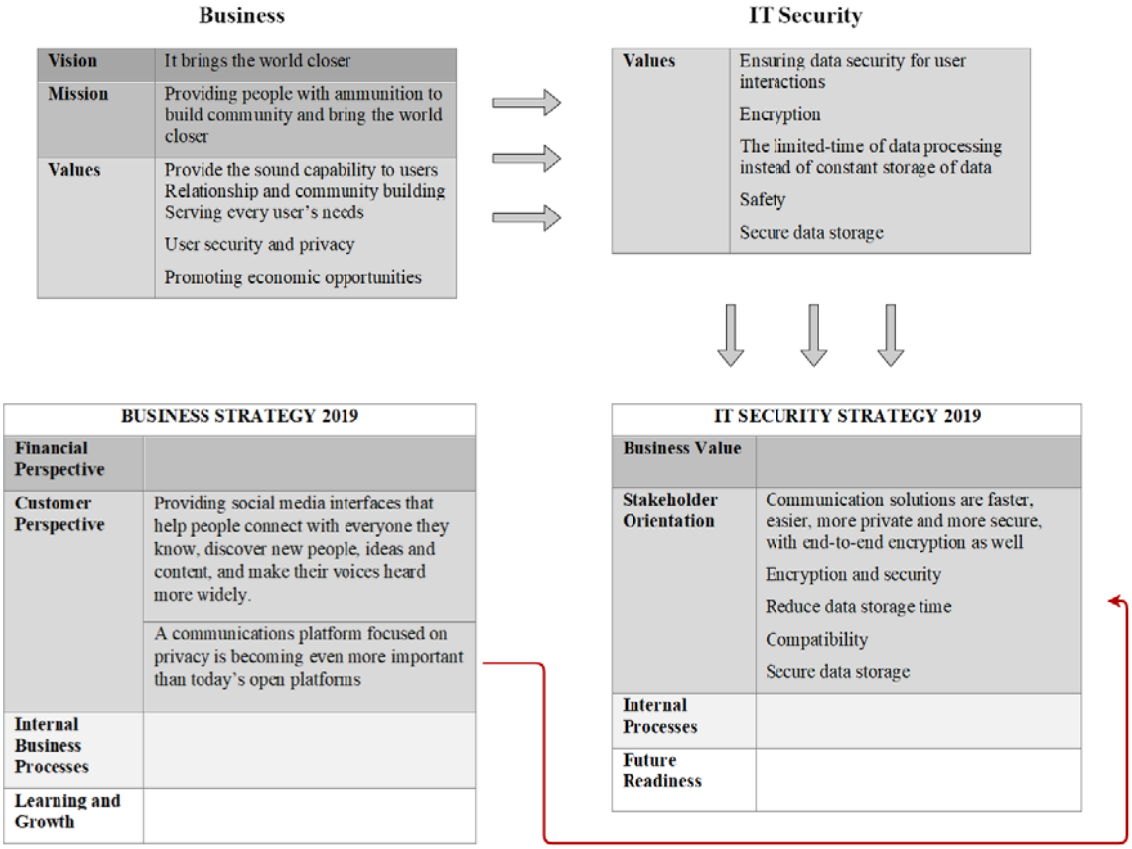

Figure no. 4: Facebook's business and IT security missions and values in 2019
(Source: Author edits using Facebook, 2020)

6. Conclusion

One consequence of technological dependence is the need and necessity to ensure the expected level of operation, the non-fulfilment of which can range from a minor negative impact to a catastrophic impact. For example, following the terrorist attacks of 11 September 2001, several of the companies involved were unable to continue their operations due to the lack or inadequacy of the business continuity and disaster recovery plan. Backup and archiving as a recovery control did not work correctly. Unfortunately, this is a phenomenon that still occurs today. However, since 2001, the services available in cyberspace, the connections and interactions between cyberspace and the physical world have increased significantly. As a result of this type of negligence, the risk of data loss and consequent business closure is even higher.

Therefore, this kind of social dependence has resulted in political will to increase cyber hygiene, causing legislation's evolution. However, a review of the policy environment and the regulatory environment shows that the regulatory environment is evolving slowly, often lagging significantly behind technological developments. Furthermore, differences in interpretation and the complexity of the wording are not

negligible problems either. An example of the latter finding is that in the event of a cybersecurity incident, there may be an obligation in the European Union to notify and cooperate with different competent authorities under Articles 6, 14 and 16 of the NIS Directive, Articles 33 and 34 of the GDPR, Article 19 of eIDAS and PSD2 under Article 19. So that, a multinational defender entity shall comply with several other requirements. Meanwhile, there is pressure to increase the efficiency of operation.

However, as an unwanted result of intense technological innovations and market competition, the recklessly implemented innovation can result in faulty design, implementation, or operation, causing an increased risk level. This phenomenon works against security, fundamentally shaking the security principles by design and privacy by designing legal requirements appearing as an increased risk factor. In this continuous development, adaptation to the dynamically changing environment is crucial to formulate the goals and their relevant metrics, which the Balanced Scorecard poses to be a helpful tool. Furthermore, with the cascade of goals, i.e., cybersecurity goals have to support business goals, this tool may help defenders to be able to choose the (at least pseudo-) proper control-mix.

As a result of intense technological innovation and market competition, defender entities may not have the necessary up-to-date capabilities to tackle the novelties. The reckless implementation of technology, the lack of knowledge about cyber-risks, and their negligence can result in faulty design, implementation, or operation, resulting in a significant risk in the entity's internal operation and its customers.

Nevertheless, due to the legal framework's continued advancement, legislation requires that defender entities apply a risk-based approach defined on the business values to be protected with development of proper control-mix comprising preventing and reactive security control. This approach may provide the optimal costs for the IT, information, or cybersecurity management system, where some incidents are taken willingly.

In contrast, others are consciously assumed, as the case studies showed. The cases provide how important a defender entity can tackle incident management and the correspondent processes and how imperative is the feedback of an occurred incident. The cases comprise the cybersecurity incidents affecting and Facebook's services.

After the identification and publicity of the incidents, Facebook drew the lessons of the incidents, the results of which he fed back into its operation through the corporate vision and mission.

Acknowledgements

This research was supported by the ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01 / 0.0 / 0.0 / 16_019 / 0000822).

REFERENCES

Alpcan, T., & Başar, T. (2010). Network security: A decision and Game-Theoretic approach. In *Network Security: A Decision and Game-Theoretic Approach*, available at: https://doi.org/10.1017/CBO9780511760778

Business Insider. (2018). *Facebook just announced it was hacked, and almost 50 million users have been affected*, available at: https://www.businessinsider.com.au/facebook-security-attack-affecting-50-million-users-2018-9

Business Insider. (2019). *Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now,* available at: https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3

Chandler, A.D. (1962). Strategy and Structure: Chapters in the History of the American. *MIT Press*.

CNBC. (2019, October 30). *Facebook stock rises on better-than-expected revenue and earnings*, available at: https://www.cnbc.com/2019/10/30/facebook-fb-q3-2019-earnings.html

Das Magazin. (2016, December 3). *Ich habe nur gezeigt, dass es die Bombe gibt*, available at: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review, Vol. 101, Issue 1*, 69–75, available at: https://doi.org/10.2478/raft-2021-0011

European Parliament and of the Council. (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council. *Journal of the European Union*.

European Parliament and of the Council. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council. *Journal of the European Union*.

Emmanuel Chukwudi, A. (2017). Game Theory Basics and Its Application in Cyber Security. *Advances in Wireless Communications and Networks*, available at: https://doi.org/10.11648/j.awcn.20170304.13

Ernst &Young. (2020). *How does security evolve from bolted on to built-in?,* available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report-single-pages.pdf

European Commission. (2012). *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM/2012/0140 final)*.

Facebook. (2019). *Keeping Passwords Secure*, available at: https://about.fb.com/news/2019/03/keeping-passwords-secure/, accessed on 10 august 2020.

Facebook. (2020). Available at: https://about.fb.com/company-info/, accessed on 30 October 2020.

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced Scorecard Implementation of Security Strategies: A Frameworkfor IT Security Performance Management. *Information Systems Management, Vol. 27, Issue 1*, 72–81, available at: https://doi.org/10.1080/10580530903455247

ISO/IEC. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*.

Kaplan, R.S., & Norton, D.P. (1992). The Balanced Scorecard-Measures that Drive Performance. *Harvard Business Review*.

Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J.P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys*, available at: https://doi.org/10.1145/2480741.2480742

Markets Insider. (2019). *Facebook shares drop sharply after unearthed emails reportedly show Mark Zuckerberg is aware of "problematic privacy practices" (FB)*, available at: https://markets.businessinsider.com/news/stocks/facebook-stock-price-reaction-to-zuckerberg-reportedly-aware-privacy-issues-2019-6-1028274446

Omalaja, M.A., Eruola, O.A., & College, I. (2011). Strategic Management Theory : Concepts, Analysis and Critiques in Relation to Corporate Competitive Advantage from the Resource-based Philosophy. *Economic Analysis*.

PCI Security Standards Council. (2018). *Payment Card Industry (PCI) – Data Security Standard – Requirements and Security Assessment Procedures*, available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

European Parliament and of the Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council, *Official Journal of the European Union.*

European Parliament and of the Council. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council. *Official Journal of the European Union*.

StatCounter. (2020). *GlobalStats*, available at: from https://gs.statcounter.com/, accessed on 27 October, 2020

Techcrunch. (2019, September 4). *A huge database of Facebook users' phone numbers found online*, available at: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/

The Guardian. (2015, December 6). *What are Facebook and other social media doing about Donald Trump?,* available at: https://www.theguardian.com/technology/2015/dec/06/donald-trump-facebook-social-media-tv

The Guardian. (2017). *Watchdog to launch inquiry into misuse of data in politics*, available at: https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump

The Guardian. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

The Intercept. (2017). *Facebook failed to protect 30 million users from having their data harvested by Trump campaign affiliate*, available at: https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/

The New York Times. (2016, November 20). *Cambridge Analytica and the Secret Agenda of a Facebook Quiz*, available at: https://www.nytimes.com/2016/11/20/opinion/cambridge-analytica-facebook-quiz.html

The Verge. (2019, March 13). *Facebook, Instagram, and WhatsApp are still down for some users around the world*, available at: https://www.theverge.com/2019/3/13/18264092/facebook-instagram-down-partially-post-messages-profile-loading

Van Grembergen, W. (2000). The balanced scorecard and IT governance. *ISACA Journal*.

von Neumann, J., & Morgenstern, O. (2007). Theory of games and economic behavior. In *Theory of Games and Economic Behavior*. Princeton University Press, available at: https://doi.org/10.2307/2019327

Wheeler, E. (2011). *Security Risk Management*. Syngress.