Land Forces Academy Review
Vol. XXVI, No. 3(103), 2021

FURTHER 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@mail.muni.cz

ABSTRACT:

In current socio-economic processes, info-communication services play a determining role, modifying the activities of certain actors. The growing dependence that has developed over the past two decades has imposed the need to give political will to security, which has led to an iterative evolution of the regulatory environment. Therefore, the regulatory framework requires certain entities to develop safeguards including controls that enhance both prevention and response in a manner commensurate with the business value of the information to be protected. However, due to the nature of cybersecurity, developing such countermeasures is not the task of a standalone organization but all entities in cyberspace in a wide range, from individuals to the public sector. Therefore, each entity involved must design protection capabilities in a manner commensurate with the risk, which requires strategic tools and methods and drives organizations to learn from their security incidents. Following our previous paper "Business strategy analysis of cybersecurity incidents" (Bederna et al.) on the topic, this paper reviews the essential formal security strategy formulation tools applied in the cases of Yahoo! and Estonia. Both are based on publicly available information. The analysis confirms the importance of managements' or the government's attitude and support for solving cybersecurity challenges.

KEYWORDS: cybersecurity, cybersecurity capabilities, cybersecurity strategy

1. Introduction

In our previous article (Bederna et al., 2021), we made a business strategy analysis for the case of Facebook. As we have shown in that research, an inevitable result of fierce technological innovation and market competition, reckless implementation of innovation can lead to errors in design, implementation, or operation, leading to higher levels of risk. This phenomenon is not conducive to security and, by designing legal requirements as a higher risk factor, it fundamentally breaks the principles of security of design and privacy. In this type of continuous development, adaptation to a dynamically changing environment is critical to setting related targets and indicators and is viewed by the balanced scorecard as a helpful

DOI: 10.2478/raft-2021-0032

tool. In addition, with the cascade of objectives, that is, cybersecurity objectives must support business objectives. This tool can help defenders choose (at least falsify) appropriate control combinations.

Due to fierce technological innovation and market competition, defensive entities may not have the up-to-date capabilities necessary to cope with developments. As a result, reckless implementation of technology, lack of knowledge of cyber risks and their negligence can lead to errors in design, implementation or operation, posing significant risks to the internal operations of the entity and its clients.

However, due to the continuous advancement of the legal framework, the legislation requires the defence entity to apply a risk-based approach, define the commercial value to be protected and develop an adequate control portfolio, including preventive and reactive security controls. This approach can provide the best cost for IT, information or network security management systems, some of which are voluntary.

On the contrary, as the case study shows, others make conscious assumptions. Cases provide the importance of advocacy entities in handling incident management and related processes and the importance of necessary feedback on incidents. These cases include cybersecurity incidents affecting Facebook's services. After identifying and publishing the incident, Facebook learned the lessons of the incident and fed its results back to its operations through its corporate vision and mission. In this paper, we show what can happen when an entity is negligent with cybersecurity. Furthermore, we present an excellent pioneer example from the European Union's cybersecurity history.

2. Case Study of Yahoo!

Yahoo! 's history, specifically its second phase, from about 2008 onwards, is a beautiful example of the combined decline resulting from poor management decisions, cybersecurity negligence, and the resulting security incidents. For this reason, it is advisable to review the incidents in the highlight of the company's life.

The company was created in March 1995, and the initial public offering was in 1996. Subsequently, Yahoo! 's share price increased by 600 per cent while continuously expanded its portfolio (Forbes, 2016). In 1999, it acquired Geocities for $3.6 billion and Broadcast.com for $5.7 billion. However, later Yahoo! failed to acquire both Google and Facebook.

In 2000, due to the dotcom bubble, the share price fell to its fraction (Forbes, 2016). In February 2008, Microsoft made a $44.6 billion takeover bid (Microsoft Corporation, 2008), which was rejected by management. After that, however, the company slowly started down the slope.

On 11 July 2012, Yahoo Voice was attacked by an SQL injection-based attack that resulted in data of 450,000 registered accounts being compromised (Techcrunch, 2012).

In August 2013, criminals stole about 3 billion user data, including user name, email address, phone number, date of birth, and password. (Yahoo! stored passwords with the application of the MD5 hash algorithm, which already provided insufficient security at that time.) However, the incident was severe due to the number of users involved and the affected data's sensitivity; it was only revealed on 14 December 2016, when the notification was about 1 billion compromised accounts (CNET, 2016). As a result of the ongoing forensic analysis, investigators revealed in October 2017 that the attack had compromised about 3 billion user account.

On 22 September 2016, the company announced that in 2014, an additional 500 million accounts had been compromised. The type of data involved was almost the same as in the previous incident. Furthermore, in the incident, public actors and employees were involved in the United States (TechRepublic, 2016). The Securities and Exchange Commission (SEC) in the US fined the company $ 35 million (US Securities and Exchange Commission, 2018) and the Information Commissioner's Office (ICO) in the UK £250,000 (approximately $180,000) (Information Commissioner's Office, 2018).

On 25 July 2016, Verizon made an offer to acquire the company's core competencies for $4.83 billion. As a result of ongoing regulatory investigations, on 21 February 2017, Verizon reduced its offer by $250 million and agreed to share responsibility with the seller for subsequent investigations and penalties. On 8 June 2017, Yahoo! 's shareholders approved the acquisition for $4.48 billion. The transaction was officially closed on 13 June (Techcrunch, 2016).

According to a court decision of 22 July 2020, customers involved in data protection incidents (individuals, small businesses) in the United States may receive $25,000 in compensation if they were directly affected by the incidents. In the absence of direct involvement, the customer could use the credit monitoring service free of charge or request a $100 cash payment, for which the company had to set up a fund worth $117 million (CNBC, 2020).

SWOT and strategy analysis

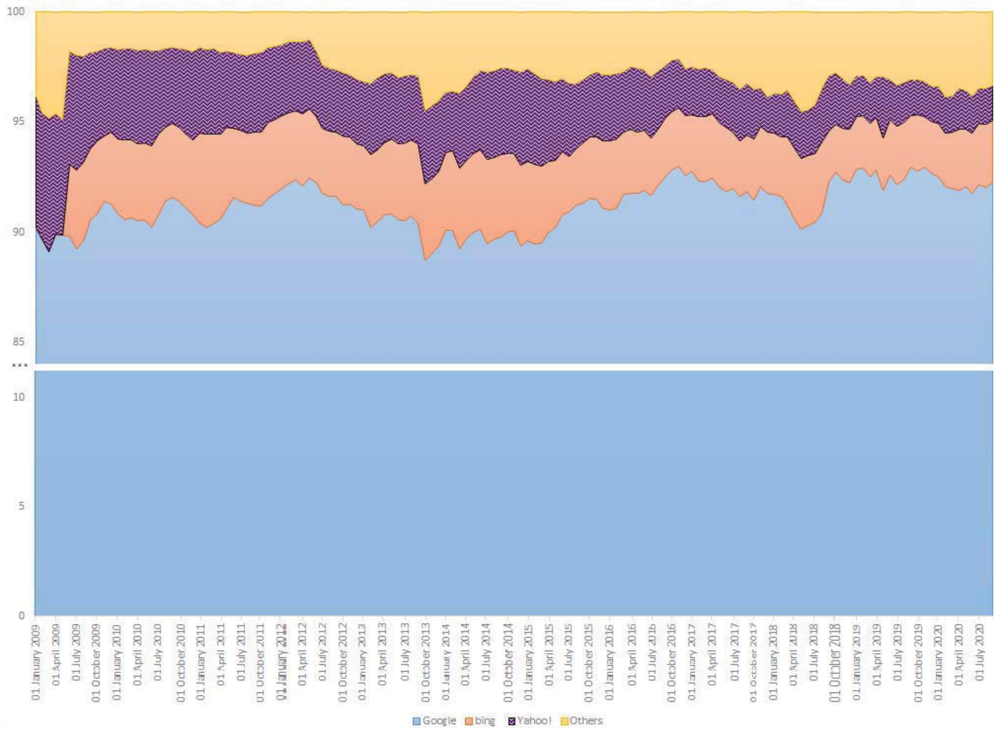
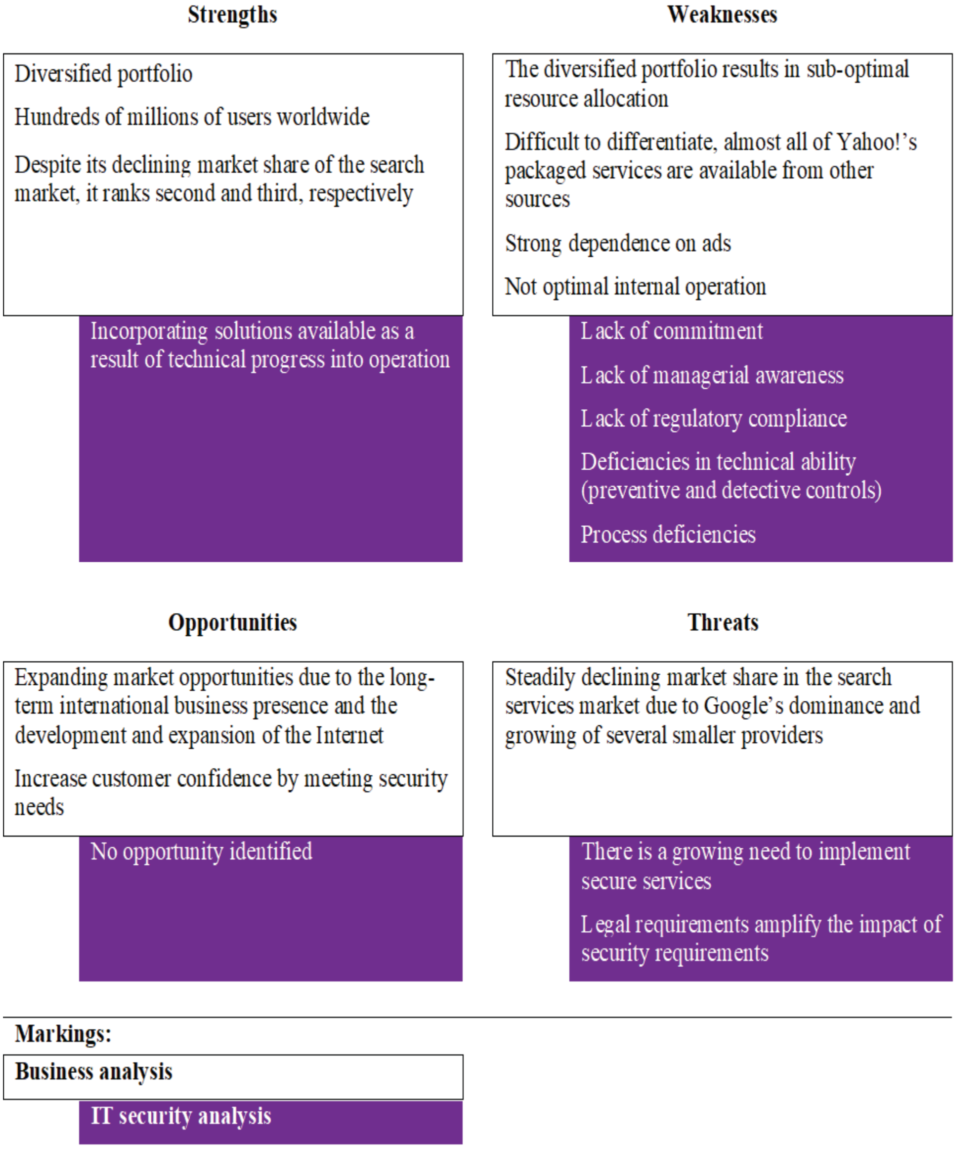


Figure no 1: *Search Engine Market Share between January 2019 and September 2020*
Source: Own edit using (StatCounter, 2020)

Yahoo! 's revenue originated from ads. However, in addition to Google's dominance, Yahoo! 's has steadily lost its market share, which was 5.91 per cent in January 2009, compared to 2.96 per cent in December 2015. This tendency continued in 2016 as well (*Figure no 1*), resulting in lower revenues. So, in 2015, Yahoo! 's annual revenue was $4,968.301 million, while its total operating expenses were $9,716.795 million, resulting in a tremendous loss.

The SWOT and strategy analysis focuses on the years 2015 and 2016 as in that time, Yahoo! recognized the incidents, notified the public, and stakeholders reacted to the information they got. Based on the obtained information, negative characteristics dominate the SWOT analysis (Figure no. 2). One of them is that much time elapsed between the occurrence and detection of the incidents and the affected users' notification. Such a delay was already unacceptable in 2014-2016 before, for example, the GDPR legislation.



Strengths

Diversified portfolio

Hundreds of millions of users worldwide

Despite its declining market share of the search market, it ranks second and third, respectively

Incorporating solutions available as a result of technical progress into operation

Weaknesses

The diversified portfolio results in sub-optimal resource allocation

Difficult to differentiate, almost all of Yahoo!'s packaged services are available from other sources

Strong dependence on ads

Not optimal internal operation

Lack of commitment

Lack of managerial awareness

Lack of regulatory compliance

Deficiencies in technical ability (preventive and detective controls)

Process deficiencies

Opportunities

Expanding market opportunities due to the long-term international business presence and the development and expansion of the Internet

Increase customer confidence by meeting security needs

No opportunity identified

Threats

Steadily declining market share in the search services market due to Google's dominance and growing of several smaller providers

There is a growing need to implement secure services

Legal requirements amplify the impact of security requirements

Markings:

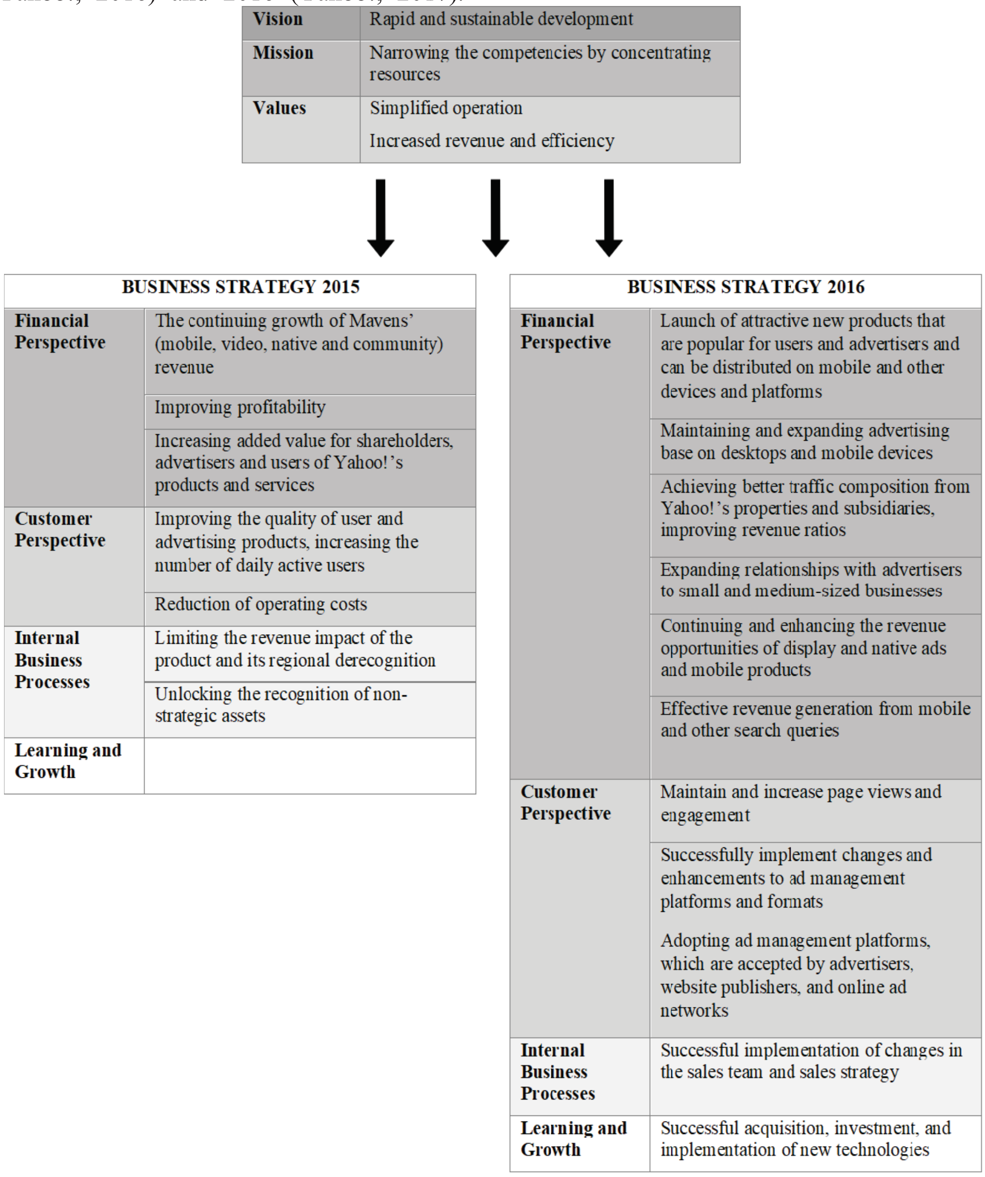
Business analysis

IT security analysis

Figure no. 2: *SWOT analysis – Yahoo! in 2015 and 2016*
Source: Own edit

The following figure (Figure no. 3) shows Yahoo! 's business strategy for 2015 and 2016. The strategy formulation uses the previous discussion and, as a plus, the relevant strategic objectives described in the annual report for Form-10K 2015 (Yahoo!, 2016) and 2016 (Yahoo!, 2017).

It is noticeable that already in 2016, Yahoo! focused on acquisitions. However, Yahoo! did not emphasize achieving safe operation despite users' mass involvement in the incidents. Hence, the company did not change its processes in order to decrease the risk.



Vision	Rapid and sustainable development
Mission	Narrowing the competencies by concentrating resources
Values	Simplified operation Increased revenue and efficiency

BUSINESS STRATEGY 2015	
Financial Perspective	The continuing growth of Mavens' (mobile, video, native and community) revenue
	Improving profitability
	Increasing added value for shareholders, advertisers and users of Yahoo! 's products and services
Customer Perspective	Improving the quality of user and advertising products, increasing the number of daily active users
	Reduction of operating costs
Internal Business Processes	Limiting the revenue impact of the product and its regional derecognition
	Unlocking the recognition of non-strategic assets
Learning and Growth	

BUSINESS STRATEGY 2016	
Financial Perspective	Launch of attractive new products that are popular for users and advertisers and can be distributed on mobile and other devices and platforms
	Maintaining and expanding advertising base on desktops and mobile devices
	Achieving better traffic composition from Yahoo! 's properties and subsidiaries, improving revenue ratios
	Expanding relationships with advertisers to small and medium-sized businesses
	Continuing and enhancing the revenue opportunities of display and native ads and mobile products
	Effective revenue generation from mobile and other search queries
Customer Perspective	Maintain and increase page views and engagement
	Successfully implement changes and enhancements to ad management platforms and formats Adopting ad management platforms, which are accepted by advertisers, website publishers, and online ad networks
Internal Business Processes	Successful implementation of changes in the sales team and sales strategy
Learning and Growth	Successful acquisition, investment, and implementation of new technologies

Figure no. 3: *Business strategy of Yahoo!*
Source: Own edit using (Yahoo!, 2016, 2017)

3. Case Study of Estonia

Case study

After regime-change, Estonia became a digitalization leader due to the pioneering eGovernment in 1997, e-ID in 2002 and e-Voting in 2005 (Kalvet, 2012), causing an increase in the number of attack vectors. By utilizing the expanded space of attack vectors, the attacker entities conducted a nationwide cyberattack campaign between 27 April 2007 and 18 May 2007 (Bederna, 2019, p. 138).

In the first few hours, the widespread attack hit both the public and private sectors forcing email services, websites, domain servers, and other services unavailable by Distributed Denial of Service (DDoS). A large number of spams charged several email accounts (Schmidt, 2013).

The rest of the campaign was separated into two phases. In the first stage, mostly script kiddies created malicious traffic that mostly had a foreign origin. This attribute made it possible, for example, to reduce the impact of an attack of DDoS-based Internet banking services by banning foreign-origin traffic – meanwhile, operators excluded real-user requests, too. After analyzing each IP address block, the given block was re-enabled if more real users' traffic and less malicious traffic were experienced to minimize the false positives.

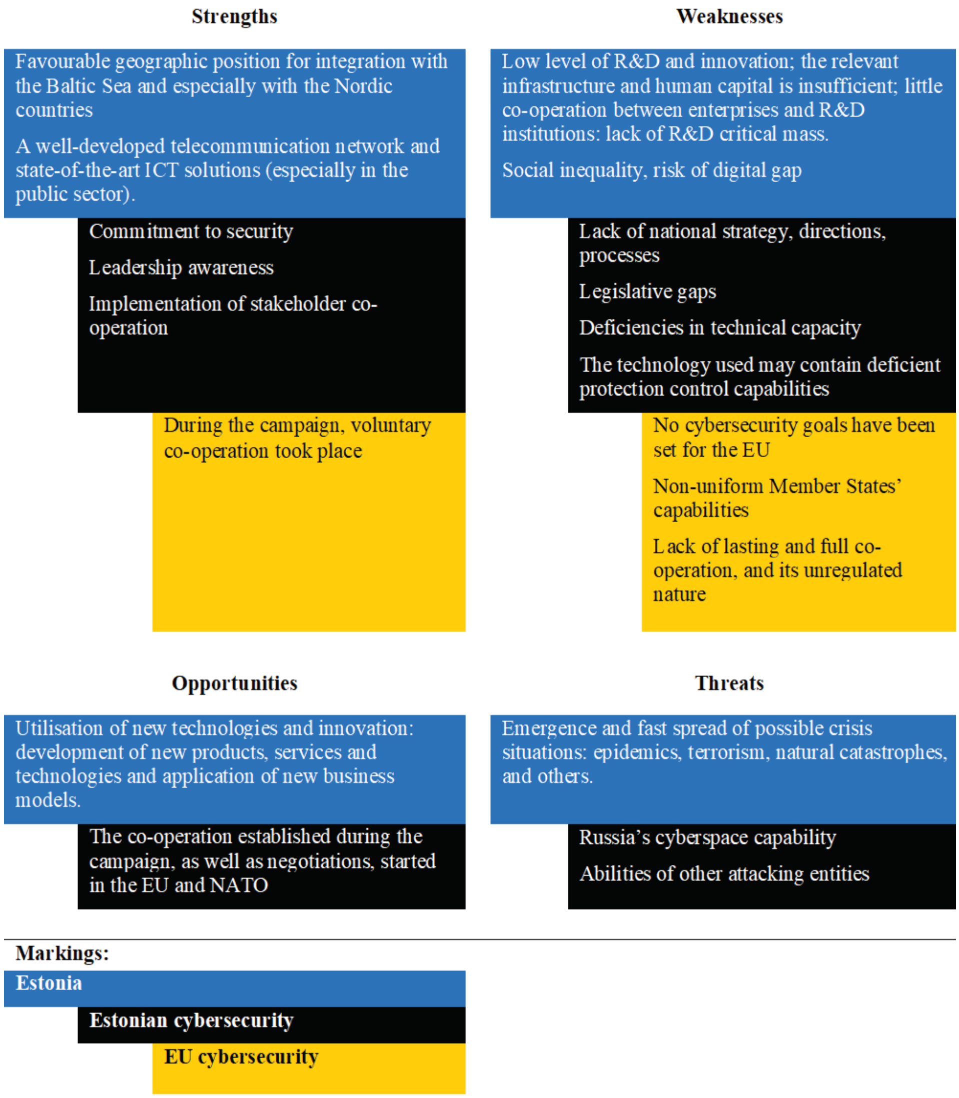
The second phase began on 30 April, in which the attackers used a more sophisticated apparatus than the first phase's attackers. So that the attacks were based on botnets, in this phase, four waves were distinguishable. The peak of the first wave was on 4 May, which reached websites and domain servers. In the second wave, mostly government and financial services were attacked between 9 and 11 May. In the third wave, government and financial services were hampered, culminating on 15 May. During the fourth wave, government and banking services were attacked again.

Although the available technical data analysis was carried out in detail during and after the campaign, the attacker entities' real identity is still in mystery; however, Russia is supposed to be behind the scenes, which declined the accusation.

During the campaign, international cooperation took place in the technological and political world. For example, several national CERTs (Community Emergency Response Team) gave investigation services (Schmidt, 2013), and ENISA (European Union Agency for Network and Information Security from 2004, European Union Agency for Cybersecurity from 2019) also offered its services. Meanwhile, NATO (North Atlantic Treaty Organisation) and the European Union started discussions about the possible enhancement of cyber defence and cyberattacks' criminality. As a result, in April 2008, NATO declared the centralization of operation in cyber-defence (Herzog, 2011), and in August 2008, CCD CoE (Cooperative Cyber Defence Centre of Excellence) was established in Tallinn. Also the case impacted a change of NATO's doctrine. (Bányász et al., 2021)

SWOT and strategy analysis

Using the previous discussion, *Figure no.* 4 presents the results of examining Estonia's national and related cybersecurity internal capabilities and external factors. In determining the national capacities and external factors, the proper SWOT analysis elements (the Republic of Estonia, 2007, p. 57) prepared by the Estonian government related to this topic served as the primary inputs. However, to be comprehensive, the analysis includes the capabilities and behaviour of the European Union attested during the campaign.



Strengths

Favourable geographic position for integration with the Baltic Sea and especially with the Nordic countries

A well-developed telecommunication network and state-of-the-art ICT solutions (especially in the public sector).

Commitment to security

Leadership awareness

Implementation of stakeholder co-operation

During the campaign, voluntary co-operation took place

Weaknesses

Low level of R&D and innovation; the relevant infrastructure and human capital is insufficient; little co-operation between enterprises and R&D institutions: lack of R&D critical mass.

Social inequality, risk of digital gap

Lack of national strategy, directions, processes

Legislative gaps

Deficiencies in technical capacity

The technology used may contain deficient protection control capabilities

No cybersecurity goals have been set for the EU

Non-uniform Member States' capabilities

Lack of lasting and full co-operation, and its unregulated nature

Opportunities

Utilisation of new technologies and innovation: development of new products, services and technologies and application of new business models.

The co-operation established during the campaign, as well as negotiations, started in the EU and NATO

Threats

Emergence and fast spread of possible crisis situations: epidemics, terrorism, natural catastrophes, and others.

Russia's cyberspace capability

Abilities of other attacking entities

Markings:

Estonia

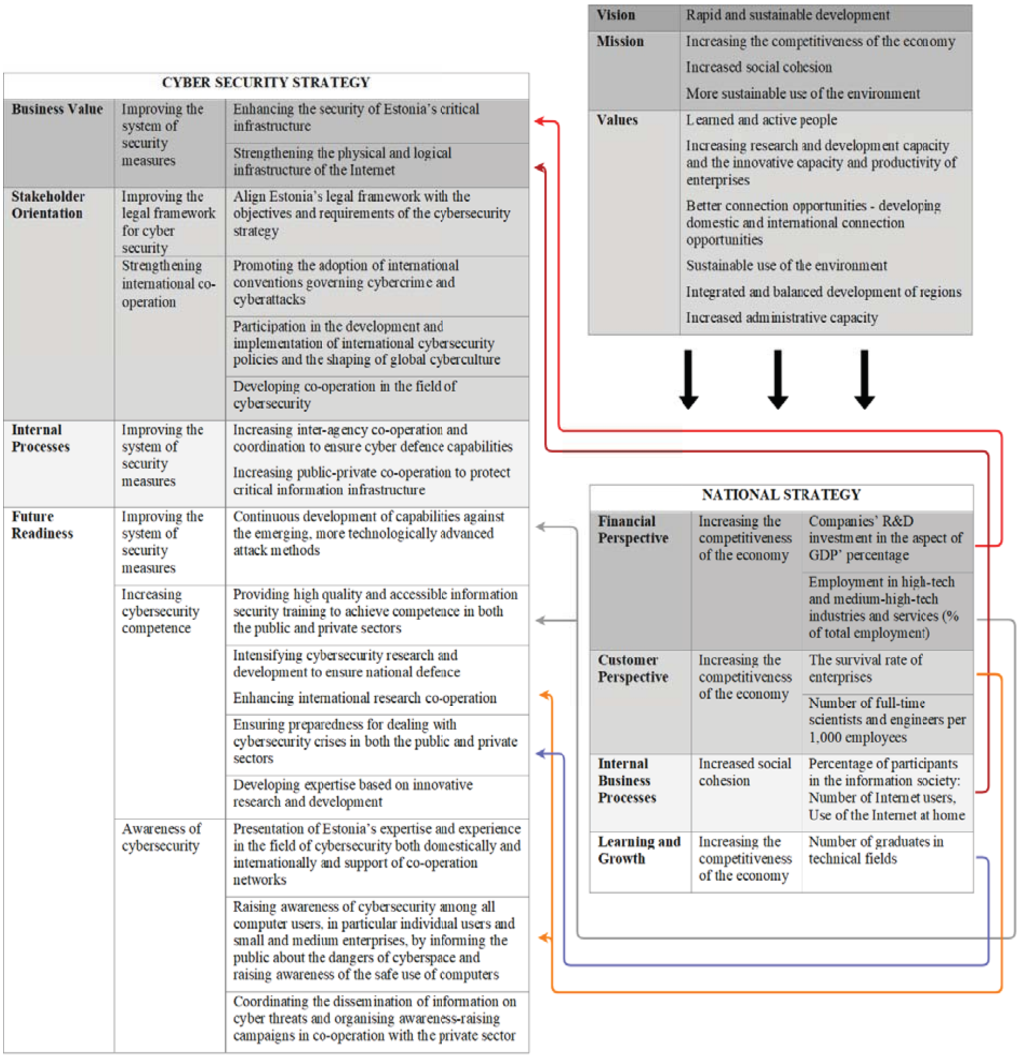
Estonian cybersecurity

EU cybersecurity

Figure no. 4: *SWOT analysis – Estonia 2007*
Source: Own edit using (Republic of Estonia, 2007)

The campaign showed that how demolishing a cyberattack can be. However, Estonian got from stuck wisely, feedbacked the learnt fact to the National Strategy (Republic of Estonia, 2007) in 2007 and the National Cyber Security Strategy (Ministry of Defence - Estonia, 2008) in 2008.

The following figure (Figure no. 5) illustrates the relationship between the National Strategy and the National Cyber Security Strategy according to the BSC.



Vision	Rapid and sustainable development
Mission	Increasing the competitiveness of the economy Increased social cohesion More sustainable use of the environment
Values	Learned and active people Increasing research and development capacity and the innovative capacity and productivity of enterprises Better connection opportunities - developing domestic and international connection opportunities Sustainable use of the environment Integrated and balanced development of regions Increased administrative capacity

NATIONAL STRATEGY		
Financial Perspective	Increasing the competitiveness of the economy	Companies' R&D investment in the aspect of GDP' percentage
		Employment in high-tech and medium-high-tech industries and services (% of total employment)
Customer Perspective	Increasing the competitiveness of the economy	The survival rate of enterprises
		Number of full-time scientists and engineers per 1,000 employees
Internal Business Processes	Increased social cohesion	Percentage of participants in the information society: Number of Internet users, Use of the Internet at home
Learning and Growth	Increasing the competitiveness of the economy	Number of graduates in technical fields

CYBER SECURITY STRATEGY		
Business Value	Improving the system of security measures	Enhancing the security of Estonia's critical infrastructure
		Strengthening the physical and logical infrastructure of the Internet
Stakeholder Orientation	Improving the legal framework for cyber security	Align Estonia's legal framework with the objectives and requirements of the cybersecurity strategy
	Strengthening international co-operation	Promoting the adoption of international conventions governing cybercrime and cyberattacks
		Participation in the development and implementation of international cybersecurity policies and the shaping of global cyberculture
		Developing co-operation in the field of cybersecurity
Internal Processes	Improving the system of security measures	Increasing inter-agency co-operation and coordination to ensure cyber defence capabilities Increasing public-private co-operation to protect critical information infrastructure
Future Readiness	Improving the system of security measures	Continuous development of capabilities against the emerging, more technologically advanced attack methods
	Increasing cybersecurity competence	Providing high quality and accessible information security training to achieve competence in both the public and private sectors
		Intensifying cybersecurity research and development to ensure national defence Enhancing international research co-operation
		Ensuring preparedness for dealing with cybersecurity crises in both the public and private sectors
		Developing expertise based on innovative research and development
	Awareness of cybersecurity	Presentation of Estonia's expertise and experience in the field of cybersecurity both domestically and internationally and support of co-operation networks
		Raising awareness of cybersecurity among all computer users, in particular individual users and small and medium enterprises, by informing the public about the dangers of cyberspace and raising awareness of the safe use of computers
		Coordinating the dissemination of information on cyber threats and organising awareness-raising campaigns in co-operation with the private sector

Figure no. 5: *National Strategy (2007) and Cybersecurity Strategy (2008) of Estonia*
Source: Own edit using (Ministry of Defence - Estonia, 2008; Republic of Estonia, 2007)

4. Conclusion

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 the 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 planning and operating processes and how imperative an incident's feedback is. The cases comprise the cyberattack campaign against Estonia and the incidents affecting Yahoo!'s and Facebook's services.

Following the cyber-attack campaign, the Estonian government was well aware of the importance of cybersecurity features, the direct industry that implements them. Accordingly, the Estonian National Cybersecurity Strategy of 2008 was five years ahead of the European Union's Cyber Security Strategy. The strategy was related to Estonia's international aspirations, technological development and society's technological dependence. During the campaign, consultations began at the international, NATO and the European Union levels to explore possible new ways to enhance cybersecurity. These efforts were successfully put to the advantage of the Estonian government, which resulted in the establishment of the NATO CCD CoE in Tallinn in August 2008.

In contrast, after the identification and publicity of the incidents, Yahoo! showed no willingness to meet the legal and social security requirements and expectations, all of which were almost entirely ignored by the management. As a result, the company's core competencies could be sold at a reduced price. Contrary to Yahoo!'s attitude, 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

Bányász, P., Krasznay, Cs., & Tóth, A. (2021). A NATO kibervédelmi szakpolitikája [NATO's cybersecurity politics] In: Szenes, Z. (ed.) *A mai NATO : A szövetség helyzete és feladatai [Today's NATO: Status and roles of the alliance]*. Budapest, Magyarország: HM Zrínyi, pp. 130-149.

Bederna, Z. (2019). Critical Information and Communications Technology protection. In Z. Rajnai (Ed.), *KIBERBIZTONSÁG-CYBERSECURITY 2.* Biztonságtudományi Doktori Iskola. Available on: https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf

Bederna, Z., Rajnai, Z., & Szádeczky, T. (2021). Business strategy analysis of cybersecurity incidents. *Land Forces Academy Review, Vol. 26, Issue 2*, 139-148.

CNBC. (2020, February 6). *If you got an email about the $117.5 million Yahoo data breach settlement, here are your options*. Available on: https://www.cnbc.com/2020/02/06/what-to-do-if-you-got-email-from-yahoo-about-a-data-breach-settlement.html

CNET. (2016, December 14). *Yahoo sets hack record at 1 billion accounts*. Available on: https://www.cnet.com/news/yahoo-hack-1-billion-users-affected-2013-record/

Forbes. (2016, July 25). *Yahoo Sells to Verizon in Saddest $5 Billion Deal in Tech History*. Available on: https://www.forbes.com/sites/briansolomon/2016/07/25/yahoo-sells-to-verizon-for-5-billion-marissa-mayer/

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*. https://doi.org/10.5038/1944-0472.4.2.3

Information Commissioner's Office. (2018). *Yahoo! fined £250,000 after systemic failures put customer data at risk*. Available on: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/06/yahoo-fined-250-000-after-systemic-failures-put-customer-data-at-risk/, accessed at 12 August 2020.

Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. *Electronic Government*. Available on: https://doi.org/10.1504/EG.2012.046266.

Microsoft Corporation. (2008). *Form 8-K*. Available on: http://edgar.secdatabase.com/2814/95012308001038/filing-main.htm

Ministry of Defence – Estonia. (2008). Cyber Security Strategy. Available on: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en

Republic of Estonia. (2007). *Estonian National Strategic Reference Framework 2007-2013*. Available on: https://www.struktuurifondid.ee/sites/default/files/estonian_national_strategic_reference_framework_2007-2013.pdf, accessed at 16 October 2020.

Schmidt, A. (2013). The Estonian Cyberattacks. In J. Healey (Ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. https://doi.org/10.1080/10803920.2014.976111

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

Techcrunch. (2012, July 12). *Yahoo Confirms, Apologizes For The Email Hack, Says Still Fixing. Plus, Check If You Were Impacted (Non-Yahoo Accounts Apply)*. Available on: https://techcrunch.com/2012/07/12/yahoo-confirms-apologizes-for-the-email-hack-says-still-fixing-plus-check-if-you-were-impacted-non-yahoo-accounts-apply/

Techcrunch. (2016, July 25). *Verizon buys Yahoo for $4.83 billion*. Available on: https://techcrunch.com/2016/07/25/verizon-buys-yahoo-for-4-83-billion/

TechRepublic. (2016, September 22). *Yahoo confirms 500M accounts leaked in massive data breach*. Available on: https://www.techrepublic.com/article/yahoo-confirms-500m-accounts-leaked-in-massive-data-breach/

U.S. Securities and Exchange Commission. (2018). *Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million.* Available on: https://www.sec.gov/news/press-release/2018-71, accessed at 12 August 2020.

Yahoo! (2016). *Form 10-K 2015*. Available on: http://www.sec.gov/edgar.shtml, accessed at 07 January 2021.

Yahoo! (2017). *Form 10-K 2016*. Available on: http://www.sec.gov/edgar.shtml, accessed at 07 January 2021.