Privacy and Cybersecurity Insights

Maria Alina Carataș
Elena Cerasela Spătariu
Gabriela Gheorghiu
"Ovidius" University of Constanta, Romania
maria.caratas@gmail.com
ebarbu2001@yahoo.com
gabrielag3110@yahoo.com

Abstract

This research paper concerns the interactions between privacy and cybersecurity as business risks, exploring how the same challenges apply to both of them and how security is a global threat in a digitalized world.

In their quest to gain competitive advantage, capitalizing on digital information and owning personal data, businesses of all types get challenged in managing risks, being exposed to data privacy and cybersecurity. As information and processes get digitized, more risks occur and an organization evolution is influenced by the way it manages risks of all kind: reputational, ethics, conformity, regulation, market, strategic, credit.

The paper raises awareness and encourages dialogue on data governance and presents important direction lines over cyber security as a fundamental part of online privacy protection.

Key words: cyber security, data privacy, data breach, risk management.
J.E.L. classification: K24, M42, M48, O33

1. Introduction

The world transformed since the digital era began, everything got more complex and can be instantly changed, with overwhelming opportunities. What seemed impossible in the past becomes a reality, life gets easier in the present with the help of technology but at the same time, we are more exposed to cyber risks.

In their quest to gain competitive advantage, capitalizing on digital information and owning personal data, businesses of all types get challenged in managing risks, being exposed to data privacy and cybersecurity. Virtual environment generated by the cyberinfrastructures and the content of information that is processed, stored or sent and the users' actions are already part of personal and professional life but security is considered far too rarely.

The new technologies, however, entail new risks that can seriously affect the individual or the organization, given that there are numerous hostile actions carried out in the cyberspace capable of affecting the availability, integrity and confidentiality of the functioning of the information systems. As information and processes get digitized, more risks occur and an organization evolution is influenced by the way it manages risks of all kind: reputational, ethics, conformity, regulation, market, strategic, credit. Many obstacles in the digital transformation process are not associated with technology but with culture, talents, good judgement, the risk appetite, risk management ability and the old technology.

2. Theoretical background. Cyber security and digital risk

Risk management is extremely important for the success of businesses. Of course, it is normal to take risks if you seek for evolution and to use social media for better-targeted marketing campaigns. But meanwhile, companies should be aware that digitizing comes with reputation and brand value risks. There are plenty of examples of how easy is to destroy a company reputation in hours.

The top companies are the ones to capitalize their customer's data preferences with various intentions, like direct marketing campaigns, creating personalized services, assessing employees performances to improve their productivity, examinating the supply chain data to increase efficiency.

The biggest example of data breach up to that date was Equifax data breach. One of the third-largest US credit rating bureaus released the news in September 2017 that private sensitive information of 147 million people from the 50 US states was exposed. They negotiated an agreement with the Federal Trade Commission and the Consumer Financial Protection Bureau up to $690 million for people claims.

One of the greatest examples of an ethics violation and leaking data is the Cambridge Analytica and Facebook data breach, that became public in 2018. The political consulting company collected and used the personal data of 87 million Facebook users in 2015 for advertising the Trump political campaign (and later in Brexit vote and Mexican elections) – more specific, they used the data to create personalized voting ads. The fine the social media network received from the Federal Trade Commission (after refusing to recognize that they were aware of the data exposure) was $5 billion and in terms of the reputation, it is difficult to say if Facebook will be able to pass over the scandal.

The Mariott data breach is another famous case of the data breach. The Chinese spy agency, communist-controlled hacked the data of 500 million guests of Mariott hotel chain in 2018. The insurance, mortgage and real estate company, First American Financial Corporation, stated in 2018 that 885 million mortgage files were leaked, dated since 2003.

Hostile actions concern mainly:

- disrupting, disabling, destroying, degrading or maliciously controlling an information system or infrastructure;
- affecting the integrity of the data or stealing restricted information. Example: sensitive data might be extracted or recovered by cyber attackers in case of loss or theft of a mobile device.

According to the Romanian National Computer Security Incident Response Team, cybersecurity refers to "the state of normalcy resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public and private resources and services, from the cyberspace. Proactive and reactive measures may include political, concepts, standards and guidelines for security, risk management, and training awareness activities, implement engineering solutions to protect cyberinfrastructure, management identity and management consequence".

Digital risk refers to entire digital behaviour that is used to ameliorate effectiveness and response to risk for all processes and decisions that include automation, for digital surveillance and warning actions. It indicates a contrived adaptation of data, all IT and analysis, processes, human resources and organizational culture. The risk function needs to stop being seen just as a protective tool but to be part of the strategic management.

Organizations use data governance as the system to manage, engage and assure data. Data comprises full or in part, an enterprise hard copy or digital assets. Defining data becomes the key process of the business and is part of data governance best practices. The trickiest thing is to get to know what data mean for the company, to be able to realize in which ways it can be used. Authors can also add any chapters and subchapters designed to help the relevance of the paper.

From the individual point of view, most frequent privacy risks exposures are:

- Geosecurity – due to our devices (mobile phones, smartwatches, sports bracelets and accessories, tablets, GPS devices, our cars navigation system);
- Social media (Facebook, email, they are all free because actually, the users are the products they promote, selling their information to companies that produce services and products guiding by their preferences and all data they provide on social networks);

- Web browsers and apps (the applications accessing our location, camera, microphone);
- Speech Software and Smart TVs (real spies);
- Shopping & Savings Cards (information is used for creating more shopping experiences based on individuals consumption habits; also the location is tracked and might be shared).

3. Three Lines of Defense Model

40 years ago the risk management function appeared, starting to be used in banks, helping them manage risks occurred in different current activities of the organizations. With time, the Three Lines of Defense Model appeared so that the responsibilities of managing risks to be clearly defined and implemented.

Figure no.1 – The Three Lines Of Defense Model

Source: The IIA data

The business departments hold the primary responsibility of risk management because from there risk are generated – this is the ***first line of defence***. The fundamental issue is knowing the risks that arise from the activity and to take the right measure to manage them. The model is based on a concept that considers the business function is the one who knows best how to handle correct risk management, considering a powerful risk culture within the organization, for the persons in charge with managing risks. According to IIA, (2019) the first line of defence is defined by functions that own and manage risk.

The ***second line of defence*** is the risk management function, responsible for supporting the business function, by creating an effective risk management environment and surveil its implementation and application by the first line of defence. The second line of defence provides opinions so that the first line of defence can use in making the best decisions and will alert the business when these decisions are not aligned with the risk principles. IIA explains the second line as functions that supervises risk management and compliance. Here are comprised the Financial Control, Security, risk management, quality, compliance, inspection. An integrated digital risk approach

The ***third line of defence*** is the internal audit that analyses the activity of the first two functions and provides an independent view over managing risk within the organization. This function reports to an audit committee (or governing body).

The interconnection of data security risks makes even greater the occurrence of other company's risks like financial, reputational and compliance. A solution to the problem would be integrating all data risk in a data governance model and engage them in the same structure with control testing and internal control, within a comprehensive approach of risks.

All lines of defence must be knowledgeable of all changes on the risk appetite vs tolerance to risk for an integrated risk approach of a business decision, risk monitoring and control. Effective risk management determines business performance, cooperation between the first two lines of defence is crucial for business growth. Managing the business in a risk-based manner implies data assets awareness and the ability to estimate quantitatively the impact of a data breach, cybersecurity attack in case of exposure to unwanted events. Capodagli (2018) agrees on the importance of work effectiveness between the second line of defence and the business partners in negotiating convenient security levels respecting the directions given by the board.

4. Risk function

To help your readers The ascent of data analytics imposes managers to be vigilant to model risk and be aware that interrelated companies might be risk contagious.

The PricewaterhouseCoopers (PWC, 2010) studied the seven key disciplines for risk function to focus on: leadership, process alignment, proactive information, enterprise risk assessment, efficiency and culture.

- Top management needs to provide leadership, promote transparent communication, assure that everyone in the company knows and acts towards company goals and support team managers to see their departments as a network, not as individual silos.
- Process alignment – synchronizing the organizational objectives, the business process objectives, strategies and performance metrics, aiming to avoid conflicts, duplications and omissions.
- Supporting employees through a proactive information delivery, offering a complete spectrum of knowledge to all business processes.
- Enterprise risk assessment – continuous auditing the risk categories and activities of the business across the way of meeting the company's objectives and evaluate the risk-adjusted returns.
- Efficiency – analyzing the root causes of risks, working sustainably, optimizing the business processes, taking advantage of opportunities, reducing the costs and boosting competitiveness.
- Culture – emphasizing the company awareness and controlling the risk appetite with the linked processes from the three lines of defence.

5. Data protection regulation

Data classification refers to the scope of data within a business and how it is linked to processes and managers. Regulations in charge of personal data and cybersecurity are fundamental in data classification. Companies that manage to classify data can also safely protect it, using programs to evaluate and identify the content of their data assets.

The European Union adopted in 2018 the General Data Protection Regulation (GDPR) that applies to all organizations that use personal data of users from EU, regardless of their location, so it applies within EU and beyond, imposing internet privacy on a global level.

The Information Commissioner's Office (ICO) decided that Equifax U.K. breached several data protection standards in the Data Protection Act 1998 (DPA 1998), counting:

- fair and lawful processing of data;
- obtaining personal data only for one or more specified lawful purpose;
- poor retention practices;
- failure to secure personal data;
- lack of legal basis for international transfers of U.K. citizens' data to the U.S.

There is no law at the federal level in the United States up to date regarding data privacy or data security.

Nevertheless, California state elaborated in 2018 the CCPA, the Californian Consumer Privacy Act, regarding data privacy, internet-focused, for Californian consumers and will take effect in January 2020. The CCPA concerns obligations and individual rights, fines for noncompliance and the right of private action.

6. Conclusions

Online exposure to risks is high in a world where every information is connected and threats become more sophisticated. Because companies tend to not publicly disclose security violations, due to reputational risk and competition concerns, there is not sufficient information about how attacks are executed, which restricts the cybersecurity work.

Companies need to implement strong governance procedures, recruit capable staff with both technical and cyber skills, connect data governance with technology and act accordingly to protect the business reputation in case of a privacy violation. Cyber breaches occur mostly because people of human errors, therefore, is important to mitigate the risks and enhance awareness on human risk management (Deloitte, 2019). In the same time way of managing digital risk is getting insured. Companies need to think from the attacker perspective, to evaluate the risk exposures and assess the worst loss that can be provoked and invest in risk insurances for most valuable assets and preventive maintenance software.

7. References

- Capodagli S., Institute of Risk Management, 2018. *Digital risk management and resilience,* [online] Available at: https://enterpriseriskmag.com/digital-risk-management-and-resiliency-part-one/ [Accessed October 2019].
- Chartered Institute of Internal Auditors, 2019. G*overnance of risk: Three lines of defence,* [online] Available at: https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/ [Accessed October 2019].
- Data Protection Act 1998 (DPA 1998), [online] Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed October 2019].
- Deloitte LLP, Dighton R., Seaborn C., Milanov D., 2019. *Beyond the hype Global Digital Risk Survey,* [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-digital-risk-survey.pdf [Accessed October 2019].
- Deloitte LLP, Risk Advisory, Mahajan R., Parthasarathy S., Jain V., 2018. *Managing Risk in Digital Transformation*, [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_managing_risk_in_digital_transformation_112018.pdf [Accessed October 2019].
- McKinsey & Company, Inc., (Harreis H., Pancaldi L., Rowshankish K., Samandari H.) & Institute of International Finance (Portilla A., Vazquez J.), 2017. *The Future Of Risk Management In The Digital Era.* [online] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era [Accessed October 2019].
- McKinsey & Company, Inc., Ganguly S., Harreis H., Margolis B., Rowshankish K, 2017. *Digital risk: Transforming risk management for the 2020s* [online] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s [Accessed October 2019].
- PricewaterhouseCoopers, 2010. *Risk and Capital Management Insights, Risk function effectiveness,* [online] Available online at https://www.pwc.co.uk/assets/pdf/fs-risk-risk-function-effectiveness.pdf
- Romanian National Computer Security Incident Response Team, *Strategia de securitate cibernetică a României,* p.7, https://cert.ro/