CYBERSECURITY ECONOMICS AND THE BENEFITS OF GDPR

Economic Analysis

June 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Introduction

As a regulatory tool ensuring the protection of personal data, the GDPR subjects the processing of personal data to security obligations:

- **The obligation to implement measures safeguarding an appropriate level of security, as set out in Article 32**; and

- **The obligation to notify the competent authority in case of a personal data breach** or, when there is a high risk, **to communicate the breach to the affected individuals**, as described in Articles 33 and 34.

The economics of cybersecurity helps explain investment decisions in cybersecurity as a trade-off between the costs of cybersecurity investment and the expected benefits of that investment. Economic literature shows that these decisions do not always lead to the socially optimal level of cybersecurity. Indeed, there are many market failures (Anderson and Moore, 2007; Cordes, 2011) related to the deeply interdependent nature of companies and individuals in cybersecurity. Cybercrime impacts not only the targeted company but also its customers and potentially other companies exposed to contagion risk.

In economics, these impacts are called **negative externalities** and are particularly problematic because a company may weigh them against its own financial interests. In this context, companies tend to have suboptimal cybersecurity investments. Regulation helps to correct these imbalances by ensuring that companies better account for cybercrime risks and adjust their cybersecurity investment decisions accordingly.

The GDPR's impact on cybersecurity goes beyond what economists call "internalization of externalities" to also address individuals' irrationality and misinformation regarding cyber risk (Lowenstein et al., 2013). Thus, raising awareness among the public and businesses about cybersecurity issues, as well as CNIL's support work in connection with the cybersecurity ecosystem (ANSSI, etc.), has also had a beneficial effect on society.

This work follows the previous CNIL publication on the economic impact of the GDPR[1], in which we called on researchers and practitioners to explore the benefits of the GDPR. Here, CNIL initiates an exploratory effort to highlight some of the GDPR's societal benefits through its positive impact on the prevention of online crimes.

Key takeaways

Personal data protection and cybersecurity are inseparable issues.

Economic theory shows that corporate self-regulation leads to insufficient investment in cybersecurity. The GDPR fills these gaps, generating economic benefits due to the security obligation.

These gains can be illustrated by a case study on identity theft, which estimates that the GDPR has generated benefits between €585 million and €1.4 billion in the EU, solely through the effect of notifying data breaches to the individuals concerned. 82% of these benefits are realized by companies.

[1] "The economic impact of GDPR, 5 years on", CNIL: https://www.cnil.fr/en/economic-impact-gdpr-5-years

I. Underinvestment by companies in data protection

1. Personal data breaches: an information asymmetry between companies and their customers

When there is a breach of personal data processed by a company, customers or employees may suffer negative consequences. For example, data obtained by criminals may be used to commit identity theft. **In the absence of regulation, this company would not be required to disclose whether a cyberattack has occurred.**

Some economic reasons may encourage companies to be transparent, as there is a risk that the breach could be revealed by a whistleblower, which would be catastrophic for the company's image and its cybersecurity investment levels. However, this reasoning seems less applicable in the case of large-scale security breaches, where the disadvantages of transparency outweigh the advantages, given the number of potentially exposed individuals. For these companies, the optimal strategy would then be to disclose a minor cyberattack but not to reveal a significant data leak (Amir et al., 2018).

In this case, **customers suffer the negative consequences of their personal data being obtained by criminals without knowing which company was responsible for the leak. The responsible company will not face reputational damage. This situation leads to underinvestment by companies in cybersecurity** because part of the damage caused by attacks does not affect the company (there is an information asymmetry) (Garcia, 2013).

In economics, information asymmetry refers to a situation where two parties do not have the same level of information in a market. For example, in the used goods market, information asymmetry exists because the seller is better informed than the buyer about the actual quality of the item. Such situations are called "market failures," where coordination through markets leads to a suboptimal outcome in terms of economic efficiency.

If there were no information asymmetry, which means, if companies were required to be transparent, individuals could know which company caused the breach and avoid entrusting their data to it in the future (Nieuwesteeg and Faure, 2018). Thus, the incentive to invest in cybersecurity would become more important for companies to avoid personal data leaks.

Empirical studies have shown that after the communication of personal data breaches, companies' stock market value declines (Acquisti et al., 2006; Bose and Leung, 2014). These negative consequences are generally small but can be particularly strong in rare cases when the cyberattack receives media coverage (Martin et al., 2017). This is a deterrent risk for companies that holds them accountable for damages caused to their customers and employees. This accountability is observed by an increase in cybersecurity investments following the implementation of the data breach notification obligation (Murciano-Goroff, 2019; Miller and Tucker, 2011). Also, when a company is at the center of a cyberattack incident, it may tend to hire cybersecurity experts to reassure investors and consumers (Bana et al., 2022). Increased cybersecurity investments reduce the probability of a successful cyberattack (Gandal et al., 2023); therefore, data breach notifications help reduce the number of personal data breaches that have negative consequences for individuals. This reduction has been estimated twice based on its impact on identity theft: one study estimated that data breach notifications cause a 6.1% decrease in identity theft (Romanosky et al., 2011), while more recent research estimates a 2.5% decrease (Bisogni and Asghari, 2020).

The mandatory notification of personal data breaches, under penalty of financial sanctions by Article 34 of the GDPR when a high risk affects the individuals concerned, is thus essential to fight against information asymmetry affecting cybersecurity.

However, mere communication of personal data breaches cannot fully address the problem of underinvestment in cybersecurity. First, if there is no equivalent alternative to the service offered by the company, the possibility for the user to switch services will not be considered credible. This is the case for certain dominant players such as, for example, social networks gathering many users. Indeed, for an individual, leaving a social network is particularly costly since it involves losing contact with other users of the network (Beknazar-Yuzbashev et al., 2024). It is therefore unlikely that a user will switch networks for cybersecurity reasons (Qian et al., 2019; Chen, 2016), which explains the necessity to also add security standards.

2. The interdependence of companies in cybersecurity as a source of coordination failure

Another reason for establishing security standards lies in the interdependence of companies regarding their cybersecurity investment decisions. The most obvious aspect of this interdependence is the risk of contagion from cyberattacks. In 2017, the malicious software WannaCry spread from computer to computer like a virus until it reached the scale of a computer pandemic costing several billion dollars.

Another illustrative example is botnets, where computers infected by hackers are then used by other hackers for various malicious purposes such as sending spam, phishing attacks, denial-of-service (DDoS) attacks, etc. Having one's computer infected therefore negatively impacts other people.

When a company decides to invest in cybersecurity, it aims to limit the damage caused by cybercrime to its own business, but it does not invest by taking into account how the risk of contagion could affect other companies (Fedele and Roner, 2022). To limit the impact of cybercrime on the entire business ecosystem, this contagion risk should be considered in cybersecurity investment decisions, which would lead to a higher investment level (Böhme, 2012).

This is a situation where positive externalities exist from cybersecurity investments. A classic example of a positive externality is beekeeping, since the producer has a positive ecological impact through their activity. When a company invests in cybersecurity, the benefits extend not only to itself but also to other companies.

Companies are also interdependent because a cyberattack impacts not only the stock market valuation of the attacked company but also that of its competitors. There are two possible types of impacts: a "spillover" effect and a "competition" effect. The competition effect is intuitive: when a company suffers a data breach, its users may want to turn to its competitors. A data breach at one company has a positive impact on its competitors. The spillover effect is more surprising because it represents the situation where a data breach at one company negatively impacts its competitors. This occurs because a cyberattack causes individuals to lower their overall security expectations of the entire sector to which the company belongs (Kelton and Pennington, 2020).

Between these two opposed effects, which one dominates depends on the scale of the data breach. When breaches are large in scale, consumers tend to consider the risk sufficiently high to move to competitors, so the competition effect prevails. When the breach is smaller in scale, customer defections are very limited; however, the "guilt by association" phenomenon persists, and the spillover effect dominates (Martin et al., 2017). The majority of personal data breaches are not large-scale and receive relatively little media coverage. Thus, in most cases, data breaches mainly produce a spillover effect and negatively affect all companies in the sector concerned by the breach (Haislip et al., 2019). This discourages investment in cybersecurity because even if a firm implements security measures to limit cyberattack impacts, it may still suffer reputational damage by association with weaker links in the sector (Nagurney and Nagurney, 2015).

The inclusion of security standards in the GDPR (Article 32) therefore benefits all companies, as it is optimal to coordinate at a high level of cybersecurity. Such coordination is impossible without regulation because companies can free-ride on the sector's overall high level of protection without bearing the costs—similar to how one benefits from herd immunity in vaccination (Su et al., 2023).

Economist Hal Varian notably demonstrated in his paper "System Reliability and Free Riding" (2001) that this framework can be modeled as a **public goods** problem. A public good is non-rival and non-excludable. A non-rival good can be consumed by multiple people simultaneously without reducing availability for others (for example: a television broadcast). A non-excludable good is one where people cannot be prevented from consuming it (for example: oxygen or street lighting).

Here, the public good is not the cybersecurity solution itself, but the resilient IT environment created by investments in cybersecurity. Such public goods are necessarily underinvested in when financed by private actors without coercive measures to punish non-participation.

Interdependence is also very strong in subcontracting relationships. When a subcontractor processes data on behalf of a data controller, the security of personal data processed by the controller also depends on the subcontractor's security level. The damage from a data breach mainly affects the data controller. This is the case for cyberattacks known as "supply chain attacks," where a cybercriminal tries to enter an organization via a subcontractor in the supply chain that has a weaker cybersecurity level. In these attacks, the weakest link in the chain determines the security level of the entire supply chain.

Due to information asymmetry, the subcontractor knows better the security level of its IT systems than the data controller. In this scenario, the data controller cannot be fully sure that the subcontractor maintains the declared level of security, which can lead the subcontractor to neglect investment in cybersecurity. Article 28(3)(c) of the

GDPR establishes the subcontractor's legal responsibility in case of inadequate security of data processing, which incentivizes the subcontractor to pay more attention to its cybersecurity level.

3. Ransomware as a market: how companies' demand affects ransom costs

Ransomware is a particularly well-known type of cyberattack. The principle is that a malicious virus blocks access to an individual's or a company's data unless a "ransom" is paid.

From the cybercriminals' point of view, how to determine the ransom amount? The optimal ransom amount is the one that maximizes their profits. If the ransom is too high, nobody will pay. Conversely, if the ransom is too low, the profits won't be significant. Choosing the optimal ransom amount thus requires the cybercriminal to consider individuals' willingness to pay.

Individuals' willingness to pay forms a demand curve: as the price increases, the number of people willing to pay decreases, which is a typical market mechanism.

A necessary consequence of this market mechanism is that the higher the ransom price, the more harmed the victims are. Indeed, if the price is low, many victims recover their data at a low cost. If the price is high, fewer victims pay, meaning more people lose their data, and those who pay lose more money. In economics, consumer surplus (here, the victims of cybercrime) decreases as price increases.

However, the price tends to be high because willingness to pay is very heterogeneous. Based on interview data, one can distinguish individuals with a very high willingness to pay and those with a low willingness to pay. Economically, it is optimal for cybercriminals to exploit those with high willingness to pay by setting a high price.

Here again, there is an externality. Individuals and companies that do not implement adequate cybersecurity measures risk being hit by ransomware, which increases the overall demand from the cybercriminal's perspective and thus drives up ransom amounts, ultimately negatively impacting society (Hernandez-Castro et al., 2020). This externality causes underinvestment in protective measures such as data backups.

4. How large is the underinvestment ?

Due to the great difficulty in obtaining databases that track cybersecurity investments, cybercrime frequency, and impacts, it is extremely challenging to estimate the gap between the current cybersecurity investment level and the optimal one.

The Gordon and Loeb model, which determines the optimal investment level for companies, was adjusted by its authors to show how the gap between optimal and actual investment changes depending on the level of externalities (the share of cybercrime damage not accounted for by the company).

Table 1
Relationship between externalities and underinvestment in the Gordon-Loeb model (2015)

Percentage of externality	Private cost of cyberattack	Optimal investment for the company	Optimal investment for society	Percentage of underinvestment
0 %	400 000 €	60 000 €	60 000 €	0 %
20 %	400 000 €	60 000 €	75 271 €	20,29 %
40 %	400 000 €	60 000 €	89 315 €	32,82 %
60 %	400 000 €	60 000 €	102 386 €	41,40 %
80 %	400 000 €	60 000 €	114 663 €	47,67 %
100 %	400 000 €	60 000 €	126 274 €	52,48 %
120 %	400 000 €	60 000 €	137 318 €	56,31 %
140 %	400 000 €	60 000 €	147 871 €	59,42 %
160 %	400 000 €	60 000 €	157 992 €	62,02 %
180 %	400 000 €	60 000 €	167 731 €	64,23 %
200 %	400 000 €	60 000 €	177 128 €	66,13 %

Gordon and Loeb show that according to their model, a company whose private cost of a cybersecurity breach is €400,000 should invest €60,000 in cybersecurity. However, if 20% of the damage are externalities, the optimal amount to invest for the community is €75,000. If externalities represent twice the company's private cost, then the optimal societal investment is €177,000.

Given the many externalities discussed earlier, it seems unlikely that the externality share is below 20%. **Therefore, the underinvestment by companies is probably in the range of 20% to 66%.**

Based on Eurostat data, the GDPR's entry into force influenced French companies' updates of cybersecurity protocols. The annual survey on IT usage in EU companies by Eurostat includes a cybersecurity section[2]. In 2015, 14.2% of French companies with at least 10 employees updated their cybersecurity protocols in the past year. This rose to 18.3% in 2019, then dropped to 12.1% in 2022. These figures show how the GDPR helped reduce underinvestment in cybersecurity.

[2] "Security policy, measures, risks and staff awareness by NACE Rev.2 activity", 2024, Eurostat. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ran2/default/table?lang=en

II. Case study: data breach communication and identity theft

To illustrate the type of benefits enabled by the GDPR, this section estimates the impact that data breach communication (Article 34) has had on identity theft. Only a relatively small portion of the gains is studied here since only the most well-known cybercrimes (Malware, DDoS) are mentioned; moreover, the impact of the presence of Data Protection Officers (DPOs, Article 37) or the establishment of cybersecurity standards (Article 32) is not discussed.

1. Direct Impact

Empirical studies in cybersecurity face many challenges due to the lack of available data to study the phenomenon (Moore et al., 2019). For example, estimations of the cost of cybercrime varies widely. In France, Statista estimates the cost of cybercrime at 119 billion euros[3], whereas the firm Astères estimates this cost at 2 billion euros in 2022[4]. These difficulties led the European Commission to develop the E-crime project, which aims to rigorously estimate the cost of cybercrime. The CNIL relies on this work to illustrate the economic gains linked to investments in cybersecurity encouraged by GDPR.

This study limits its analysis to the impact on identity theft because it is the cybercrime offense with the best-documented cost. However, it must be kept in mind that this is only one form of cybercrime. The gains reflected by the GDPR here likely represent only a small portion of the total gains in cybercrime prevention since it is difficult to document, due to a lack of data, those related to other forms of cybercrime (such as ransomware, for example). It should also be noted that it seems easier to focus on the impacts on individuals, but cyberattacks also have consequences on the productivity or reputation of companies, which are not accounted for here. For example, Derichebourg announced on April 16, 2024, that it had suffered a cyberattack that rendered its operating software unavailable. This attack caused a slowdown in its activity, resulting in losses estimated between 15 and 20 million euros.[5]

This document also focuses on the impact of breach notifications. Indeed, the impact of other GDPR provisions on cybersecurity has, it seems, not yet been treated in economic literature. The GDPR also contains security obligations for the processing of personal data in its Article 32 (pseudonymization, impact analysis, etc.).

Since this study only aims to examine part of the GDPR's impact on cybersecurity, the estimates presented here may be a lower bound of the total GDPR gains in cybersecurity. Data breach notification to individuals is an older rule, notably implemented in the United States in the early 2000s, which explains why its impact has been more strongly studied by economists.

Identity theft occurs when a cybercriminal uses personal information obtained about a person to impersonate them. Four types can be distinguished following the typology of Riek and Böhme (2018), whose work was funded by the European Commission's E-crime project. The four types of identity theft studied are: theft where the criminal gains access to a bank account (IDT_OB), access to credit card information (IDT_BC), access to a PayPal account (IDT_PP), and access to an online shopping account (IDT_OS). This represents only part of the identity theft cases impacting affected individuals. These identity thefts have an average cost in monetary loss and time loss for the individual (to obtain reimbursements, replace identifiers, change cards, etc.).

The data from Riek and Böhme on the cost of cybercrime were obtained via questionnaires with 6,394 individuals from various European countries (Italy, Germany, Estonia, Poland, Netherlands, United Kingdom), which allows including unreported cybercrimes. The table below presents the average monetary and time costs of identity theft reported by individuals in 2018, shown with a 90% confidence interval[6]. It can be noted that the wide confidence intervals reflect the highly variable nature of cybercrime cost, which is often very low or even zero but can occasionally be very high, so the median loss is lower than the average loss.

[3] « *Le coût de la cybercriminalité explose en France* », 2024, Statista. Available on: https://fr.statista.com/infographie/31783/cout-annuel-cybercriminalite-cyberattaques-en-france/

[4] « *Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022* », Asterès. Available on : https://asteres.fr/etude/les-cyberattaques-reussies-en-france-un-cout-de-2-mdse-en-2022/

[5] « *Suite à une cyberattaque, Derichebourg perd 15 à 20 millions d'euros* », 2024, Usine Digitale. Available on: https://www.usine-digitale.fr/article/suite-a-une-cyberattaque-derichebourg-perd-15-a-20-millions-d-euros.N2211635

[6] Which means that there is 90% likelihood that the average cost of identity theft in Europe is contained in the interval.

Table 2
Cost of identity theft

Type of identity theft	Monetary cost (euros) $(\bar{C})$	Time lost (hours) $(\bar{T})$	Share of identity theft (%)
IDT_OB	[203 – 1396]	[6,2 – 10,1]	20%
IDT_BC	[250 – 534]	[6,9 – 11,2]	34%
IDT_PP	[170 – 1034]	[7,3 – 9,6]	15%
IDT_OS	[23 – 133]	[5,6 – 8,5]	29%

From these costs, it is possible to estimate the average loss per individual in a country due to cybercrime by the following formula, where α is an indicator that converts time lost into monetary cost:

$$\mathcal{L}_{IDT} = \sum_{i \in \{IDT\}} \bar{p}_i(\bar{C}_i + \alpha \bar{T}_i)$$

Using Eurobarometer 2015, an approximate probability of being a victim of identity theft can be estimated at 8% in the EU [7](which is consistent with Riek's approach) and 9% in France. For the estimate of α, it is possible to base it on the median wage in France and the EU in 2018[8]. Finally, the GDPR impact this study focuses on is the impact of data breach notifications. The impact of such a policy on identity theft has been studied twice in the economic literature. Romanosky (2011) found a 6.1% decrease in identity theft cases, and Bisogni (2020) found a 2.5% decrease following the implementation of a data breach notification policy. These two figures can be used to estimate the GDPR's impact on the average cost per individual of identity theft:

$$GDPR\ Gains = Nb\_Internet\_Users\ (\mathcal{L}_{Pre\_GDPR} - \mathcal{L}_{Post\_GDPR})$$

To find the number of internet users over 18 years old in the EU and in France, we can use the percentage of individuals using the internet in 2018[9] [10], along with data from INSEE on the age distribution in France [11]and from Eurostat in the EU[12]. From these data, it is possible to estimate that the cost of identity theft in France ranges between 1 and 3.4 billion euros over 4 years. In the EU, this figure is between 6 and 15 billion euros.

Table 3
Direct costs of identity theft avoided by data breach notification (in millions euros)

	2.5 % decrease	6.1 % decrease
European Union	**405**	**988**

[7] « Europeans' attitudes towards cyber security », European Union. Available on: https://europa.eu/eurobarometer/surveys/detail/2171
[8] « Low-wage earners as a proportion of all employees (excluding apprentices) by sex », 2021, Eurostat: https://doi.org/10.2908/EARN_SES_PUB1S
[9] *Baromètre du numérique 2018* (PDF, 5,6 Mo), Arcep. Available on: https://www.arcep.fr/uploads/tx_gspublication/barometre-du-numerique-2018_031218.pdf
[10] « World Bank Indicators », World Bank. Available on: https://databank.worldbank.org/source/world-development-indicators
[11] « *Pyramide des âges – projections de population 2021 – 2070 – Scénarios* », Insee. Available on: https://www.insee.fr/fr/outil-interactif/5896897/pyramide.htm#!y=2018&a=60,70&v=2&g&t=1&c=0
[12] « Population on 1 January by age and sex », Eurostat, https://doi.org/10.2908/DEMO_PJAN

	[189,7 – 620]	[463 – 1512]
France	**54** [25,4– 83]	**132** [62 – 205,5]

It can thus be concluded that GDPR has helped avoid between 54 and 132 million euros of losses linked to the direct costs of identity theft in France, and between 405 and 988 million euros of losses at the EU level.

Riek's questionnaire also contained information on compensation amounts paid to individuals by companies or insurance firms, allowing to determine how much loss individuals and companies respectively avoided. On average, 70% of the losses caused by identity theft are compensated by companies. In France, individuals avoided between 16 and 40 million euros of losses, and companies between 39.5 and 96 million euros. At the EU level, individuals avoided between 105 and 257 million euros of losses, and companies between 164 and 402 million euros.

2. Indirect impact

So far, this study has ignored indirect costs, which are an important part of the costs caused by cybercrime. Indirect costs affect society as a whole and can be attributed to the impact cybercrime has on individuals' confidence in the security of online activities where sensitive data must be transmitted (e.g., credit card information), resulting in reduced business revenue. Riek, Böhme, and Moore (2015) show that individuals' confidence in the security of their personal data online is strongly affected by their past experiences with cybercrime. The impact also affects society by ch. For example, a Belgian study (Paoli and Visschers, 2017) estimates that 5.9% and 10.4% of the population have limited their use of online banking and e-commerce respectively due to cybersecurity risks. In the 2018 ARCEP digital barometer, 29% of respondents declared hesitation to shop online due to payment security concerns. Anderson et al. (2019) estimate indirect costs of payment fraud at $1.6 billion in the UK.

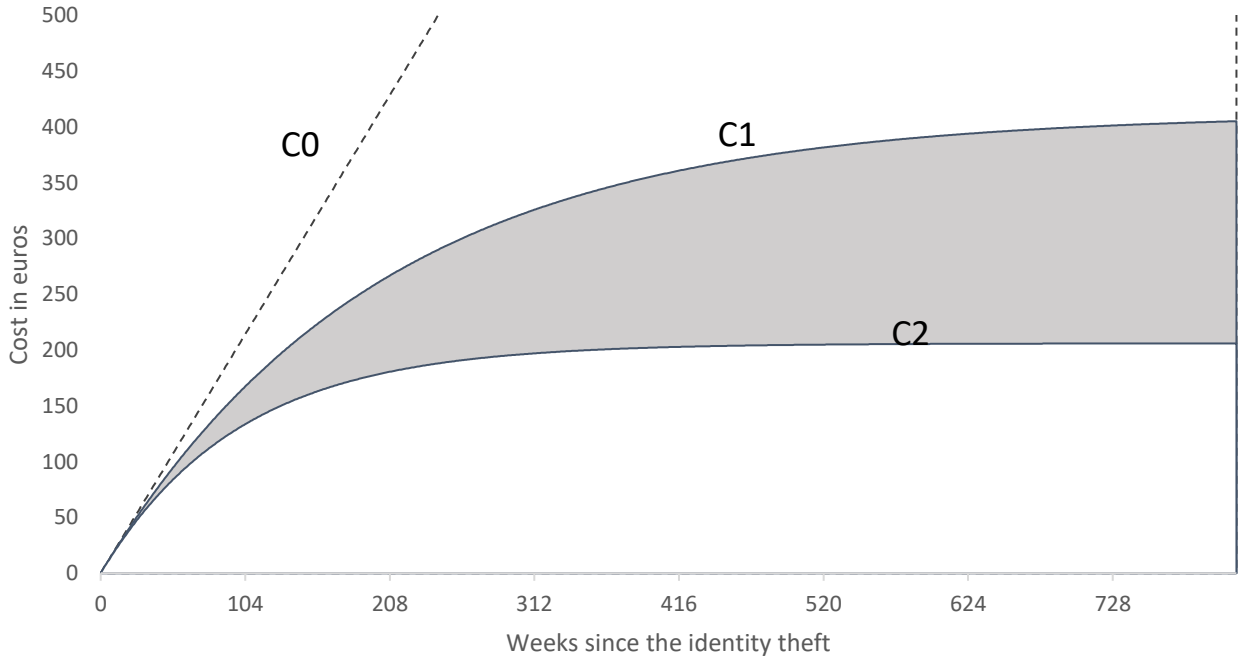
As one can imagine, if the direct cost of cybercrime is complex to estimate, estimating indirect costs is even more difficult. To attempt to estimate indirect costs, Riek and Böhme (2018) collaborated with a German credit card provider to observe how individuals' transaction behaviors changed after they experienced credit card identity theft (IDT_BC). The author then surveyed part of the population to understand how their buying habits changed. Results show a large share of individuals become cautious and significantly reduce the number of online transactions, which is not fully compensated by an increase in offline purchases. Specifically, the average number of weekly online transactions drops from 1.32 to 1.02 after identity theft. Comparing pre- and post-event behavior, the author estimates the indirect cost for the sector at 2.06 euros per week for this form of cybercrime.

However, the study has a limitation: individuals were only followed for 18 weeks after the theft, during which no trend toward normalization was observed. It seems unrealistic that individual behavior changes permanently, but it is not known when habits return to normal. To compensate, this study assumes the impact of cybercrime on individual behavior decays over time, modeled as a geometric series with a depreciation rate λ.

$$Indirect\ Loss = \sum_{i=1}^{\infty} \lambda^{i-1} 2{,}06$$

There appears to be no economic literature estimating this depreciation rate. However, given the significant psychological impact of cybercrime on victims, potentially causing disorders such as PTSD (Bada and Nurse, 2020; Kirwan and Power, 2012), and the long lifespan of identity theft where leaked personal data can be repeatedly reused by criminals to open bank accounts or take out loans, it seems reasonable to assume that psychological impact persists for several years. This analysis proposes two λ values: in the first, the impact decreases by 0.5% per week ($\lambda 1$), and in the second, it decreases twice as fast, by 1% per week ($\lambda 2$). The following graph illustrates the cost function shapes for these parameters.

Figure 1
Indirect costs of credit card identity theft (IDT_BC)



Note : 104 weeks ≈ 2 years.
C0 represents the undiscounted cost (unrealistic assumption that psychological impact never fades).
C1 represents the indirect cost with depreciation rate λ1.
C2 represents the indirect cost with depreciation rate λ2.

Using these models and Riek's estimate (2015), it is possible to estimate the indirect cost of credit card identity theft (IDT_CB) between 206 and 412 euros, or between 52% and 105% of the direct monetary impact of cybercrime. Due to the similarity between credit card identity theft and other identity theft types discussed, it seems reasonable to assume that indirect costs are of the same order of magnitude for other cases.

By adding indirect costs to the previously estimated function L, it is possible to re-estimate the average GDPR gains from Table 2, now including indirect costs.

Table 4
Total costs of identity theft avoided by breach notification (in million euros)

	2.5 % decrease	6.1 % decrease
European Union	**585** [509,8 – 660]	**1427** [1244 – 1610]
France	**90** [78,5– 101,2]	**219** [191 – 247]

Note: The interval represents the estimate with λ1 and λ2 ([est_λ1 – est_λ2]). The bold figure is the average of these estimates.

It can thus be concluded that GDPR has helped avoid between 90 and 219 million euros of losses linked to the total costs of identity theft in France, and between 585 and 1427 million euros of losses at the EU level. Since indirect costs are only borne by companies, it is possible to add them to the direct costs compensated by companies to obtain the total losses avoided by these companies**. It is estimated that 82% of these avoided losses concern companies.**

Conclusion

Economic research allows considering cybersecurity as an investment decision for companies. In economic theory, this choice is made by companies with the aim of maximizing their profit. These investments have effects on individuals and other companies, which are not taken into account by companies in their investment decisions. When a company invests in cybersecurity, this has a positive effect on its partners, competitors, clients, and employees. The GDPR encourages companies to invest more in cybersecurity to limit the impact of cybercrime at the societal level, thus presenting a benefit for all actors.

It is possible to estimate those benefits: the GDPR would have helped avoid losses of at least between 90 and 219 million euros in France solely through the impact of breach notification (Article 34). Over four types of identity theft, at the EU level, this provision would have helped avoid losses between 585 million and 1.4 billion euros. This is a preliminary figure aiming mainly to illustrate the potential gains of the GDPR rather than to fully account for them. Indeed, due to limitations in available data, it is difficult to provide a rigorous estimate of other cybersecurity gains enabled by the GDPR. For example, some gains were omitted from the analysis. Regarding breach notifications, one essential element was omitted: the impact of the GDPR on the average cost of identity theft. One of the core principles of breach notification is to enable the individual to take appropriate preventive measures to avoid damages which would reduce the average cost of identity theft.

Also, article 32 GDPR requires companies to implement appropriate security measures for personal data such as encryption. According to the IBM "Cost of a Data Breach 2023[13]" report, encryption reduces the average cost of a security breach by 5% and represents a basic security measure that is inexpensive to implement. It is also necessary to consider the impact of data the minimization principle (Article 5.1.c GDPR), which helps reduce the consequences of data breaches for individuals. Indeed, companies that minimize data collection are less likely to suffer data breaches with severe impact on individuals, since they do not hold sensitive information they had no reason to collect in the first place. Similarly, the storage limitation principle (Article 5.1.e GDPR) gradually reduces duration for which personal data is stored by the company, thereby lessening the negative impact of cyberattacks since companies no longer hold information about long-past clients.

All these GDPR impacts could lead to reducing the average cost of cyberattacks (i.e., the figures in Table 1), which was not taken into account in the present case study since the GDPR gains were based solely on reducing the frequency of cybercrimes. There therefore remains a whole range of gains linked to the reduction of the average cost of cyberattacks enabled by the GDPR to investigate.

The GDPR and CNIL's work related to the cybersecurity ecosystem help raise awareness among the public and companies, especially SMEs, about cybersecurity issues, which is another way regulation can help reduce the impact of cybercrime. The reduction in the impact of cybercrime could also, through its indirect effect on the online trust climate, facilitate the emergence of innovative services that heavily rely on user trust.

Many avenues remain to explore to understand the positive impact of the GDPR in the field of information security. Reports such as those from CESIN or Spiceworks mention that the GDPR has led to increased investments in cybersecurity, but the scale of this increase remains undetermined. What is the GDPR's impact on the adoption of encryption, anonymization, awareness-raising measures? How have these impacts affected the cost and frequency of cybercrime? These questions remain open and it is important that the scientific community tackles them to provide precisely quantified insights.

References

ACQUISTI, Alessandro, FRIEDMAN, Allan et TELANG, Rahul, 2006, « Is there a cost to privacy breaches? an event study. », *ICIS 2006 proceedings*, p. 94.

AMIR, Emir, LEVI, Shai, and LIVNE, Tsafrir, 2018, « Do firms underreport information on cyber-attacks? evidence from capital markets. » *Review of Accounting Studies*, 23, pp. 1177–1206.

ANDERSON, Ross, BARTON, Chris, BÖHME, Rainer, CLAYTON, Richard, GAÑÁN, Carlos, GRASSO, Tom, LEVI, Michael, MOORE, Tyler, et VASEK, Marie, 2019,« Measuring the changing cost of cybercrime », *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*.

[13] « Cost of a Data Breach Report », IBM Security. Available on: https://github.com/jacobdjwilson/awesome-annual-security-reports/blob/main/Annual%20Security%20Reports/2023/IBM-Cost-of-a-Data-Breach-Report-2023.pdf

ANDERSON, Ross and MOORE, Tyler, 2007, « The economics of information security: A survey and open questions. », *Fourth bi-annual Conference on the Economics of the Software and Internet Industries*, pp. 19–20.

Arcep. *Baromètre du numétique*, 2018. Available on: https://www.arcep.fr/uploads/tx_gspublication/barometre-du-numerique-2018_031218.pdf

BADA, Maria, et NURSE, Jason R.C., 2020, *The social and psychological impact of cyberattacks*, pp. 73–92.

BANA, Sarah, BRYNJOLFSSON, Erik, JIN, Wang, STEFFEN, Sebastian, et WANG, Xiupeng, 2022, « Human capital acquisition in response to data breaches. », *SSRN*.

BEKNAZAR-YUZBASHEV, George, JIMENEZ DURAN, Rafael, et STALINSKI, Mateusz, 2024, « A model of harmful yet engaging content on social media. » *SSRN*.

BISOGNI, Fabio et ASGHARI, Hadi, 2020, « More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Communication Laws. », *Journal of Information Policy*, Vol. 10, pp. 45–82.

BÖHME, Rainer, 2012, « Security audits revisited. », *International conference on financial cryptography and data security*, Springer, pp. 129–147.

BOSE, Indranil et LEUNG, Alvin Chung Man, 2014, « Do phishing alerts impact global corporations? A firm value analysis. » *Decision Support Systems*, Vol. 64, pp. 67–78.

CHEN, Jiawei, 2016, « How do switching costs affect market concentration and prices in network industries? » *The Journal of Industrial Economics*, 64(2), pp. 226–254.

CORDES, Joseph J., 2011, « An overview of the economics of cybersecurity and cybersecurity policy. » *CSPRI Report*, pp. 1–18.

Commission européenne et Direction générale de la migration et des affaires intérieures, 2017, *Europeans' attitudes towards cyber security*. European Commission. Available on : https://europa.eu/eurobarometer/surveys/detail/2171

Eurostat, 2012, « Low-wage earners as a proportion of all employees (excluding apprentices) by sex. ». DOI : https://doi.org/10.2908/EARN_SES_PUB1S

Eurostat, 2023, « Population on 1 january by age and sex. ». DOI : https://doi.org/10.2908/DEMO_PJAN

FEDELE, Alessandro, et RONER, Cristian, 2022, « Dangerous games: A literature review on cybersecurity investments. », *Journal of Economic Surveys*, 36(1), pp. 157–187.

GANDAL, Neil, MOORE, Tyler, RIORDAN, Michael, et BARNIR, Noa, 2023, Empirically evaluating the effect of security precautions on cyber incidents. *Computers & Security*, Vol. 133, 103380.

GARCIA, Michael E., 2013, *The economics of data breach: Asymmetric information and policy interventions*. The Ohio State University.

HAISLIP, Jacob Z., KOLEV, Kalin, PINSKER, Robert, et STEFFEN, Thomas, 2019, « The economic cost of cybersecurity breaches: A broad-based analysis. », *Workshop on the economics of information security (WEIS)*, Vol. 9.

KELTON, Andrea S., et Pennington, Robin R., 2020, « Do voluntary disclosures mitigate the cybersecurity breach contagion effect? », *Journal of Information Systems*, 34(3), pp. 133–157.

KIRWAN, Grainne, et POWER, Andrew, 2012, *The Psychology of Cyber Crime: Concepts and Principles*.

LOEWENSTEIN, George, JOHN, Leslie et VOLPP, Kevin G., 2013, « Using decision errors to help people help themselves. », *The Behavioral Foundations of Public Policy*.

MARTIN, Kelly D., BORAH, Abhishek et PALMATIER, Robert W., 2017, « Data privacy: Effects on customer and firm performance. » *Journal of marketing*, 81(1), pp. 36–58.

MILLER, Amalia R. et TUCKER, Catherine E., 2011, « Encryption and the loss of patient data. », *Journal of Policy Analysis and Management*, 30(3), p.. 534–556.

MOORE, Tyler, KENNEALLY, Erin, COLLETT, Michael et THAPA, Prakash, 2019, « Valuing cybersecurity research datasets. », *18th Workshop on the Economics of Information Security (WEIS)*.

MURCIANO-GOROFF, Raviv, 2019, « Do data breach disclosure laws increase firms' investment in securing their digital infrastructure. », *Workshop on the Economics of Information Security*, pp. 1–39.

NAGURNEY, Anna et NAGURNEY, Ladimer S., 2015, « A game theory model of cybersecurity investments with information asymmetry. » *NETNOMICS: Economic Research and Electronic Networking*, 16, pp. 127– 148.

NIEUWESTEEG, Bernold et FAURE, Michael, 2018 « An analysis of the effectiveness of the eu data breach communication obligation. » *Computer Law & Security Review*, 34(6), pp. 1232–1246.

PAOLI, Letizia et VISSCHERS, Jonas, 2017, « The impact of cybercrime on belgian businesses », *KU Leuven Centre for IT & IP Law Series*.

QIAN, Xiaofei, PEI, Jun, LIU, Xinbao, ZHOU, Mi et P. M. Pardalos, 2019, « Information security decisions for two firms in a market with different types of customers. », *Journal of Combinatorial Optimization*, 38, pp. 1263–1285.

RIEK, Markus et BÖHME, Rainer. *Towards a Robust Quantification of the Societal Impacts of Consumerfacing Cybercrime*. Universitäts- und Landesbibliothek Münster, 2018.

RIEK, Markus, BOHME, Rainer et MOORE, Tyler, 2015, « Measuring the influence of perceived cybercrime risk on online service avoidance. », *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp. 261– 273.

RIEK, Markus et BÖHME, Rainer, 2018, « The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates », *Journal of Cybersecurity*, Vol. 4, 1.

ROMANOSKY, Sasha, TELANG, Rahul et ACQUISTI, Alessandro, 2011, « Do data breach disclosure laws reduce identity theft? », *Journal of Policy Analysis and Management*, 30(2), pp. 256–286.

Su, Yiqing, Zhang, Xiaoting & Zhang Shifei, 2023, « The impact of collective action dilemma on vaccine hesitancy: Evidence from China ». *Human Vaccines & Immunotherapeutics*, 19(2):2256041.

The World Bank. World development indicators. 2024, available on: https://databank.worldbank.org/source/world-development-indicators