MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE
Liberté Égalité Fraternité

Tresor-Economics

No. 295 • December 2021

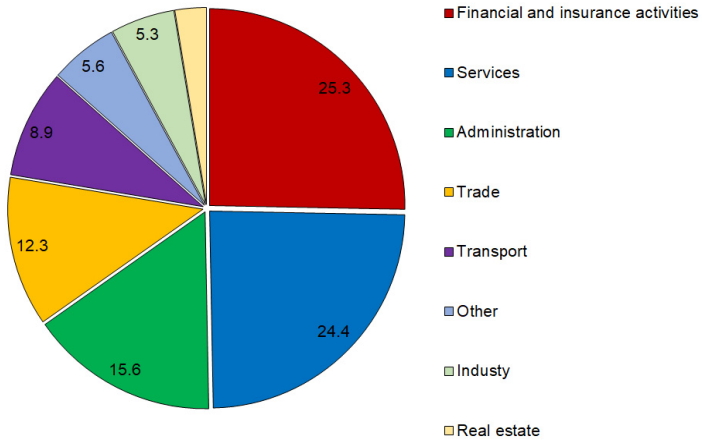
Direction générale du Trésor

Cyber Risk in the Financial Sector

Benjamin Hadjibeyli, Adrien Moutel

- Cyber risk – which encompasses all risks that arise from using digital technology – represents a major economic risk in today's world. It can be defined as an operational risk affecting the confidentiality, availability or integrity of information or information systems. It covers both malicious acts and inadvertent incidents caused by human error or accident.
- The number of cyber incidents is sharply on the rise, but the costs they represent for the economy as a whole remain difficult to estimate. There are both direct and indirect costs, affecting not only the organisation targeted by an incident but other stakeholders as well (partner firms, customers). They likely amount to several hundred billion euros annually for the global economy.
- The financial sector is a particularly attractive target for cyber attacks due to the potential for a large payoff. It is also a highly digitalised sector, which increases its exposure. During the COVID-19 pandemic, the sudden shift to work-from-home arrangements made it one of the most exposed industries.
- The financial sector is also highly interconnected, which increases the likelihood of shocks spreading more widely. To function properly, it relies on the confidence of its participants, and this confidence can be eroded by a security incident. Although a systemic event has yet to occur, cyber risk has been identified as one of the main risks for financial stability.
- Organisations tend to underestimate cyber risk and underinvest in cybersecurity. To ensure an adequate level of security, various public policy levers can be mobilised: training, regulation, stress testing, industrial policy, cyber insurance. The proposed Digital Operational Resilience Act (DORA), at the European level, and the cyber insurance working group launched by the Directorate General of the Treasury, in France, contribute to that effort.

COVID-19-related cyber events by sector (March-September 2020)



Source: Aldasoro et al. (2021), "COVID-19 and Cyber Risk in the Financial Sector".
Data mostly from US sources.

1. Cyber risk encompasses all risks that arise from using digital technology

1.1 A risk with evolving boundaries

Generally speaking, cyber risk refers to all risks associated with using digital technology. There is not a single definition for the concept, as it is relatively new and its boundaries are still evolving. A workable definition is one put forward by Cebula and Young (2010),[1] which has since been adopted by other academic studies and international standards:[2] cyber risk is an operational risk to information and technology assets that have consequences affecting the confidentiality, availability or integrity of data or information systems. Other properties, such as authenticity, can also be threatened.[3] Cybersecurity consists in protecting these properties using a security system.

Cyber risk includes both malicious and inadvertent acts: in addition to cybercrime, it includes disruptions to digital activities caused by physical risks (fire, blackout) and human error (bad code, mistakes, carelessness).

Different taxonomies have also been put forward. The one proposed by the Bank for International Settlements classifies cyber risks based on four dimensions:

- Causes: There are numerous causes or methods, and they change as technology advances. There is a relatively well-known list of unintentional causes that is not prone to change: programming errors (e.g. a bug introduced with an update), social engineering or physical risks associated with natural disasters. Intentional methods employed by malicious actors, however, tend to evolve quickly: malware (malicious software installed without consent, such as ransomware), phishing (attempts to steal confidential data by purporting to be a trustworthy source), denial of service (DoS) attacks (which seek to render a service unavailable), man-in-the-middle attacks (where attackers intercept communications, e.g. over a public Wi-Fi network) and zero-day exploits (attacks against a software vulnerability that has yet to be patched).[4]
- Actors: There are a variety of possible actors, whether internal or external to the targeted organisation. External actors include States, State-sponsored groups and criminal organisations, as well as lone hackers. A "crimeware as a service" market has also developed, where malicious tools and software are now available online for purchase by criminals.
- Intent: The main distinction to make here is whether a cyber incident is malicious (for financial or political gain) or inadvertent.
- Consequences: These can vary and are not limited to financial losses. A cyber incident can have a lasting reputational impact on a targeted organisation and cause significant external collateral damage[5] (after a data breach, for example). The severity of consequences can also vary widely: at the one end, there are the ubiquitous cyber risks of everyday work and life that have a limited impact ("routine" cyber risks); at the other, there are "black swan" events that occur rarely but with potentially catastrophic consequences.

1.2 A risk that is difficult to quantify but almost certainly on the rise

Cyber risk is difficult to quantify, due to both its evolving boundaries and a lack of transparency around cyber incidents. Measuring the risk requires knowing how frequently it occurs (i.e. the number of cyber incidents) and its potential economic impact.

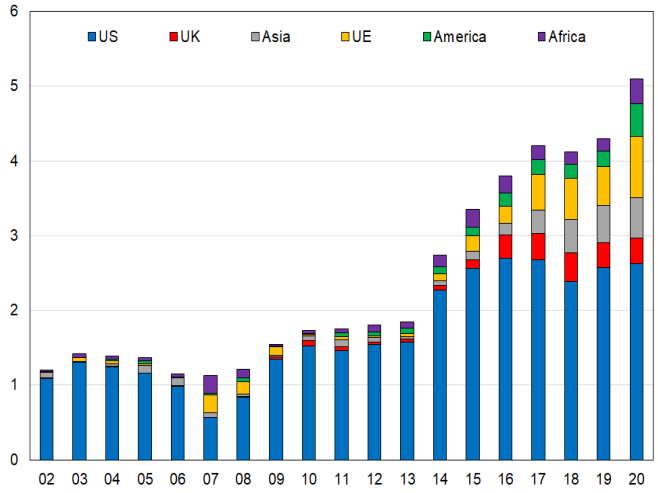
There is consensus, however, that cyber risk has considerably increased in recent years, and this has

(1) Cebula and Young (2010), "A Taxonomy of Operational Cyber Security Risks", *Software Engineering Institute Technical Note CMU/SEI-2010-TN-028*, Carnegie Mellon University.
(2) See for example Eling and Wirfs (2016), "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class", *Université de Saint-Gallen*. See also the Financial Stability Board's Cyber Lexicon.
(3) *Confidentiality* is the property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. *Integrity* is the property of accuracy and completeness. *Availability* is the property of being accessible and usable on demand. *Authenticity* is the property of the source of information being verifiable.
(4) Zero-day vulnerabilities are those that have not been publicly disclosed or fixed, which means hackers can exploit them without the knowledge of the software's users or even its vendor. In practice, such attacks are typically "n-day" attacks, where a vulnerability has been disclosed but the fix has not yet been deployed or installed for all users.
(5) In May 2021, for example, the attack on Colonial Pipeline led to panic buying at US petrol stations, causing the President to declare a state of emergency

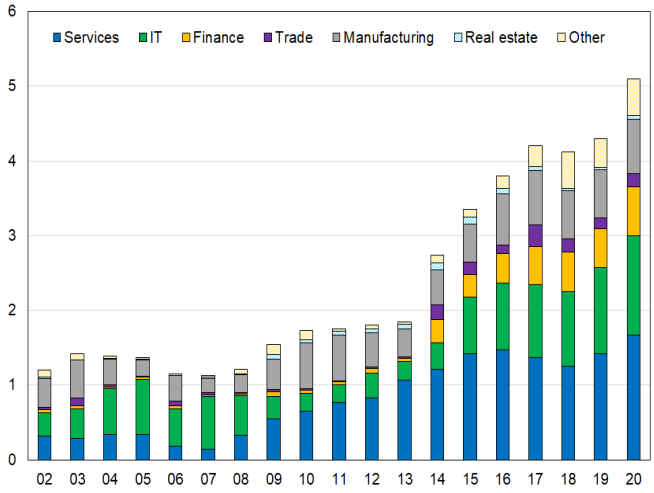
been documented in the academic literature. Using natural language processing methods on transcripts of corporate earnings calls, Jamilov et al. (2021) show that mentions of cyber risks are on the rise and the sentiment surrounding cyber risk is becoming increasingly negative.[6] By analysing the development of cyber risk by region and industry, the authors show that the risk began growing in the United States before spreading to other parts of the world (see Chart 1A) and mainly concerns the professional services sector (which includes cybersecurity service providers) and the IT sector. Their analysis also suggests that cyber risk has risen sharply in the financial sector (see Chart 1B). By examining the causes and costs of cyber incidents between 2002 and 2018, Aldasoro et al. (2020) show there has been a significant increase in the number of incidents, although the average cost remains low. Both the costs and causes of cyber incidents are highly sector-specific. For example, the financial sector is one of the most affected by such incidents, but with lower average costs, which the authors attribute to higher investment in cybersecurity.[7]

Chart 1: Cyber risk over time

A. By region



B. By industry



How to read these charts: Both charts show the proportion of quarterly earnings calls mentioning one or more cyber risk terms (as a percentage of the total number of words in each transcript), aggregated by region and industry.
Source: Jamilov et al. (2021).

Cyber risks affect firms in different ways, the first of which is a direct financial impact, such as a ransom payment or a loss of revenue due to an operational shutdown. A cyber incident can also have indirect impacts, for instance by damaging the reputation of the targeted firm, which are difficult to measure. Several studies on listed companies show that when a company discloses a cyber incident, it is followed by a negative stock price reaction.[8]

Cyber incidents can also have indirect impacts on third parties: a loss of confidence affecting the entire sector, a loss or alteration of data used by multiple firms, a ripple effect along the entire value chain caused by the shutdown of a single firm, or a long-lasting increase in risk aversion.

Several studies have made attempts to estimate the aggregate impact of such direct and indirect impacts, with widely varying orders of magnitude. In 2018, the European Systemic Risk Board (ESRB) reported estimates ranging from $50bn to $650bn.[9] McAfee and the Center for Strategic & International Studies, a think tank, estimate the impact to be nearly $1tn in 2020, or over 1% of global GDP.[10]

Some studies have sought to estimate the distribution of possible impacts, using the concept of value-at-risk (VaR): in addition to the expected average loss, this approach seeks to estimate a realistic probable loss (achievable with a probability of 5% or 10%). In a methodological exercise comparing several methods used in the literature, Dreyer et al. (2018) show the high

(6) Jamilov, Rey and Tahoun (2021), "The Anatomy of Cyber Risk", *NBER Working Paper* 28906.
(7) Aldasoro, Gambacorta, Giudici and Leach (2020), "The Drivers of Cyber Risk", *BIS Working Papers* 865.
(8) See Amir, Levi and Livne (2019), "Do Firms Underreport Information on Cyber-attacks? Evidence from Capital Markets", Review of Accounting Studies, and Tosun (2021), "Cyber Attacks and Stock Market Activity", *International Review of Financial Analysis* 76.
(9) European Systemic Risk Board (2020), "Systemic Cyber Risk", *ESRB Reports*.
(10) McAfee and Center for Strategic and International Studies (2020), "The Hidden Costs of Cybercrime".

degree of uncertainty surrounding these estimates and the high sensitivity to model parameters, obtaining estimates of average annual cost ranging from $275bn to $3.2tn (direct impacts) and from $800bn to $10.1tn (total impact). An alternative VaR method yields upper-bound estimates of $6.6tn (direct impact) and $22.5tn (total impact), or a 5% VaR of roughly one-third of global GDP.[11] In the financial sector, Bouveret (2018) estimates the average annual loss associated with cyber attacks worldwide to be roughly 10% of banks' net income (around $100bn), or as high as 30% in a severe scenario (double the number of cyber attacks that occurred in 2013).[12]

2. Cyber risk particularly affects the financial sector and could threaten financial stability

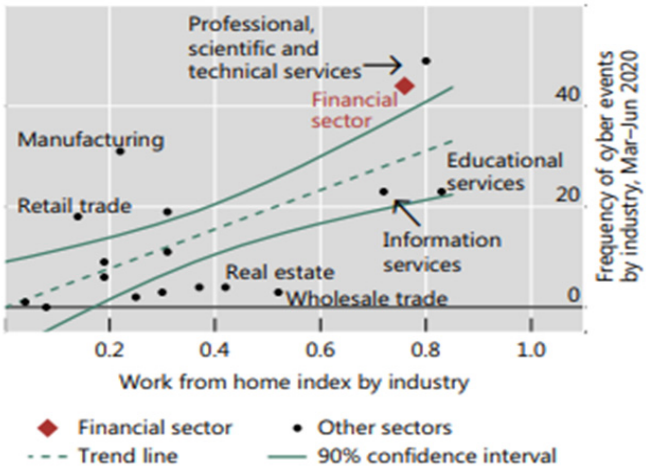
2.1 The financial sector is often a target

According to the Boston Consulting Group, financial sector firms are 300 times more likely to be targeted than those in other sectors.[13] Most academic studies identify the financial sector as one of the most targeted sectors for cyber incidents. It was also particularly exposed during the pandemic, due to the sudden and widespread shift to working from home in response to COVID-19 (see chart on cover page). The fact that the financial sector is highly digitalised makes it that much more of a target,[14] with the primary market infrastructure (for payments, settlement, clearing, etc.) being fully electronic, as well as a large portion of banking activity (securities trading, retail banking). Although the sector has seen some significant attacks in recent years, like the Carbanak malware attacks or the cyber heist targeting the Bangladesh central bank,[15] it has yet to experience a systemic incident.

Box 1: A problem aggravated by the COVID-19 pandemic

The surge in people working from home in response to the COVID-19 pandemic heightened firms' cyber risk by increasing their exposure to attacks. With firms forced to make a quick shift to digital operations in a short period of time, it was more difficult for them to maintain cybersecurity standards. One of the first actions taken to allow more people to work from home was equipping them with the tools needed to do so, including remote desktop protocol (RDP) and virtual private network (VPN) technologies; but these were the source of numerous incidents. Aldasoro et al. (2021)[a]) show a strong relationship between the prevalence of work-from-home arrangements (WFH index) by sector and the frequency of cyber attacks in Q2 2020 (see Chart 2). The risk is expected to remain high in the medium term, assuming work-from-home arrangements remain common.

Chart 2: Frequency of cyber events and WFH index by sector



Source: Aldasoro et al. (2021), "COVID-19 and cyber risk in the financial sector".

a. Aldasoro, Frost, Gambacorta and Whyte (2021), "COVID-19 and cyber risk in the financial sector", *BIS Bulletin* 37.

(11) Dreyer et al. (2018), "Estimating the Global Cost of Cyber Risk", *Research Reports RR-2299-WFHF*, Rand Corporation.
(12) Bouveret (2018), "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment", *IMF Working Papers* 18/143.
(13) Zakrzewski et al. (2019), "Global Wealth 2019: Reigniting Radical Growth", Boston Consulting Group.
(14) For example, the OECD ranks it as a digital intensive sector. Calvino (2018), "A Taxonomy of Digital Intensive Sectors", *OECD STI Working Paper* 2018/14.
(15) Between 2003 and 2018, the Carbanak malware attacks saw criminals steal more than $1bn from a hundred-odd banks across more than 40 countries. In 2016, a group of hackers exploited vulnerabilities in the SWIFT international payments network to break into Bangladesh's central bank, stealing nearly $100m.

2.2 Cyber risk could become systemic

Due to its highly interconnected nature, the financial sector is exposed to contagion risk. The financial system includes systemically important entities, primarily banks and insurers, which are highly interconnected and among whom a large proportion of assets and flows are concentrated. That means an isolated incident involving a single entity in the financial sector has the potential to spread more widely, even across borders.

To study the potential impact of a cyber incident on the financial sector, some studies have used an approach similar to that used in stress testing: they estimate the financial capacity of an organisation to absorb a substantial shock. For example, Duffie and Younger (2019) show that the 12 largest US banks reportedly have enough liquid assets to withstand a severe cyber incident.[16] Conversely, Eisenbach et al. (2020) estimate that a significant cyber incident, defined as a single-day shutdown of a bank's ability to process payments, could have a critical impact on the entire financial system if it were to occur at one of the top five US banks.[17]

The financial sector is also unique in that it depends heavily on the confidence of its participants in the security of the system. The ESRB studied how a cyber incident might threaten financial stability.[18] Various events could evolve into a systemic crisis (see Box 2). For example, an attack causing the irrecoverable destruction, alteration or encryption of data held by a financial institution could cause sufficiently serious financial losses or operational disruptions to lead to an erosion of confidence in the financial system, triggering a bank run or a liquidity freeze on the interbank market.

Box 2: Hypothetical systemic cyber incidents (ESRB[a])

- Scenario 1 (non-malicious incident): an update accidentally disrupts the payments system of a systemically important bank, preventing individuals and businesses from accessing their accounts and carrying out transactions. The incident is compounded by social media rumours of a cyber attack, leading to a widespread loss of confidence in the payments system.
- Scenario 2 (malware attack): a cyber attack unleashes a massive set of simultaneous transactions on the accounts of a major bank, altering account balances. The attackers, having previously gained access to the bank's systems for several months, also compromised its data backups and restoration processes. For a long period the bank is unable to process financial transactions, and it is unable to recover its data in the short term.
- Scenario 3 (man-in-the-middle attack): a malware is used to alter the information provided by market data providers and a central clearing house, causing trades to be rejected and incorrect price and position to be disseminated. Uncertainty spreads among market participants as to the accuracy of the information they are receiving, causing market liquidity to drop, participants to return to bilateral trading and investors to quickly unwind uncertain positions.

a. See ESRB (2020), "The making of a cyber crash".

Analysis of these different elements suggests that a cyber incident that is both malicious in nature and quick to spread widely could become systemic. It would depend on the nature of the threat: a cyber attack launched with the intent to destabilise the financial system, as opposed to for mere financial gain, could be more likely to cause a loss of confidence. It would also depend on the functions that were affected: an incident causing a permanent loss of data integrity (or appearing to do so) would be more likely to lead to a systemic event. As for transmission channels, the probability of a cyber incident having a systemic impact would be much higher if it led to a loss of confidence. Lastly, the probability of a systemic event is lower if firms and authorities are well prepared for an attack. For all these reasons, in September 2021, the High

(16) Defined as a 75% cumulative runoff of deposits over 30 business days. See Duffie and Younger (2019), "Cyber Runs", *Hutchins Center Working Paper* 51.
(17) Eisenbach, Kovner and Lee (2020), "Cyber Risk and the US Financial System: A Pre-Mortem Analysis", *Federal Reserve Bank of New York Staff Report* 909.
(18) European Systemic Risk Board (2020), "Systemic Cyber Risk".

Council for Financial Stability (HCSF), the French macroprudential authority, reiterated the importance of implementing adequate prevention and protection measures to address cyber risk, and of conducting regular crisis management exercises.[19]

3. Public policy measures are needed for the sector to properly protect itself against cyber risk

3.1 A number of market failures could lead to underinvestment in cybersecurity

There are a number of market imperfections warranting public policy measures.[20] Firstly, a misalignment of incentives could arise between those responsible for cybersecurity and those benefiting from it. This kind of misalignment often occurs between firms and their customers, with firms attempting to strike a balance between returns (digitalisation, cost savings) and user security. For example, banks encourage their customers to use online services to reduce their operational costs, but they do not incur the full cost of security flaws.

Cybersecurity is also a field where there is a high degree of information asymmetry. While it may be easy to identify a security flaw, it is impossible to prove that a system is secure. A firm may therefore be reluctant to disclose a security breach, fearing a hit to its reputation. The result is a market where it is difficult to assess the quality of the products offered by cybersecurity service providers, and therefore difficult for purchasers to distinguish between them.

Cybersecurity also generates a number of externalities. In some cases, these can be beneficial. Externalities caused by cyber risk are nevertheless usually negative, either due to the spread of the threat (e.g. via sub-contracting)[21] or through economic transmission channels (reputational loss in the sector, shutdown of a service). Accordingly, safeguarding the security of operators of essential services (OES) could limit the potential harm to society as a whole if one of these entities were to be compromised. It is therefore reasonable for the government to intervene to ensure they are resilient.

Aldasoro et al. (2020)[22] find that, on average, firms underinvest in cybersecurity, except for certain industries, including finance. However, the model used in their analysis estimates the optimal amount of spending at the firm level[23] and does not account for potential externalities.

In terms of labour, there appears to be a worldwide shortage of skilled workers in the cybersecurity sector. Some 70% of firms in the sector report a lack of specialists in their organisation, and 45% of them consider the situation to have worsened over the past few years.[24] In addition to vacancies, there seems to be a misalignment of skills in staffed positions, with many employees in the sector coming from other IT fields or having less than three years' experience in the field.

3.2 Several policy levers can be mobilised

These market failures suggest that public policy measures could be introduced to limit the effects.

First, regulation could be used to make the cybersecurity market more efficient. For example, it could realign incentives between firms and their customers by requiring firms to be responsible for the security of their customers' data. Regulation could also reduce information asymmetry by requiring firms to report cybersecurity incidents.[25] And it could develop certification schemes, like the one introduced at the European level by the Cybersecurity Act, which aims to harmonise the methods used to assess the level of protection offered by cybersecurity products. Such certification schemes can help client firms to assess the

(19) HCSF press release, 14 September 2021.
(20) See Moore (2010), "The Economics of Cybersecurity: Principles and Policy Options", *International Journal of Critical Infrastructure Protection*.
(21) Particularly involving cloud service providers, an area where a significant portion of the risk is concentrated.
(22) Aldasoro, Gambacorta, Giudici and Leach (2020), "The Drivers of Cyber Risks", *BIS Working Paper* 865.
(23) In the model, IT security investment is calibrated on the basis of a cost-benefit analysis using data from real-life incidents.
(24) Enterprise Strategy Group (2021), "The Life and Times of Cybersecurity Professionals in 2020". However, North America is overrepresented in the study sample (92%), with only 4% of firms based in Europe.
(25) See the FSB's October 2021 report "Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence".

quality of competing products. Also at the European level, the proposed Digital Operational Resilience Act (DORA) for the financial sector has a similar aim, seeking to improve incident reporting, strengthen prescriptive protection measures and impose security requirements on providers of critical services (cloud services in particular).

Second, authorities could improve their crisis response and management as well as risk assessment capabilities through stress testing. The proposed DORA will also allow for stricter stress testing requirements. Authorities could also develop specific protection systems for entities deemed to be systemically important from a digital perspective, like operators of essential services. Awareness-raising (i.e. training employees) is another essential part of building resilience to cyber risk, since human factors are a major weak point in IT systems security.

Third, as for any highly innovative activity, building up cybersecurity capabilities generates positive externalities for society as a whole that could not be internalised by cybersecurity service providers, causing them to underinvest in R&D. An industrial policy incentivising R&D could be introduced to solve this issue. Such a policy could be supplemented by training programmes to develop skills, which are essential in human-capital-intensive fields like cybersecurity, where recruitment challenges are also known to exist. That is one of the objectives of the cybersecurity plan announced last year by the French government, and a priority of the France 2030 investment plan.[26]

Lastly, private insurance mechanisms for cyber risk could help reduce these market failures by having firms internalise the risk via the cost of insurance premiums and by imposing security standards. Cyber risk insurance mechanisms have long been recommended by economists, but in practice the market remains underdeveloped.[27] There are several factors behind this failure to take off. First, there is limited demand for this type of insurance, as most firms are unaware of the existence or extent of the risk they are exposed to. On the supply side, insurance offerings are underdeveloped, as cyber risk is difficult for insurers to quantify due to incomplete, non-standardised and immature data. These factors, and particularly the high information asymmetry between insurers and policyholders, make cyber risk difficult to insure. Furthermore, cyber risk is characterised by highly interdependent risks and a dependence on large firms, which makes such highly correlated risks potentially quite costly to insure.[28] To gain a better understanding of these difficulties, and to accompany the development of this market, the French Treasury launched a national consultation on cyber risk insurance in 2021.

(26) See the France Relance press kit "Cybersécurité, faire face à la menace : la stratégie française".
(27) MacColl, Nurse and Sullivan (2021), "Cyber Insurance and the Cyber Security Challenge", *Royal United Services Institute for Defence and Security Studies Occasional Paper*. According to a recent study by AMRAE, a French association for corporate insurance and risk management, 8% of French mid-sized firms are insured against cyber risk. See "Lumière sur la cyberassurance", May 2021.
(28) See for example Granato and Polacek (2019), "The Growth and Challenges of Cyber Insurance", *Chicago Fed Letter* 426, Federal Reserve Bank of Chicago.

Publisher:
Ministère de l'Économie, des Finances, et de la Relance
Direction générale du Trésor
139, rue de Bercy
75575 Paris CEDEX 12

Publication manager:
Agnès Bénassy-Quéré

Editor in chief:
Jean-Luc Schneider
(01 44 87 18 51)
tresor-eco@dgtresor.gouv.fr

English translation:
Centre de traduction
des ministères économique
et financier

Layout:
Maryse Dos Santos
ISSN 1962-400X
eISSN 2417-9698

Derniers numéros parus

December 2021

No. 294 Economic Assessments of Services Provided by Biodiversity
Vincent Bouchet, Clémence Bourcet, Eléonore Cécillon, Sophie Lavaud

November 2021

No. 293 Labour Market Discrimination: How Is It Measured and What Is Its Economic Cost?
Cyprien Batut, Chakir Rachiq

No. 292 China's Position Among Lenders in Sub Saharan Africa
Louis Bertrand, Sary Zoghely

https://www.tresor.economie.gouv.fr/Articles/tags/Tresor-Eco

Direction générale du Trésor

@DGTrésor

To subscribe to *Trésor-Éco*: tresor-eco@dgtresor.gouv.fr