Solvency ii Association
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.solvency-ii-association.com

Solvency 2 News, January 2021

Dear members and friends,

Today we will start with EIOPA's opinion on the 2020 review of Solvency II.

Legal basis

1.1 On 1 January 2016, Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II Directive) entered into application.

1.2 The Solvency II Directive provides that certain areas of the Directive should be reviewed by the European Commission (Commission) at the latest by 1 January 2021, namely:

• long-term guarantees measures and measures on equity risk,

• methods, assumptions, and standard parameters used when calculating the Solvency Capital Requirement standard formula,

• Member States' rules and supervisory authorities' practices regarding the calculation of the Minimum Capital Requirement,

• group supervision and capital management within a group of insurance or reinsurance undertakings.

1.3 Article 77f(2) of the Solvency II Directive requires EIOPA to provide technical advice to the Commission in the form of an opinion on the assessment of the application of the long-term guarantees measures and measures on equity risk.

At the request of the Commission, the scope of EIOPA's Opinion is wider than that provided for in the Solvency II Directive.

1.4 EIOPA provides this Opinion to the Commission in accordance with Article 16a of Regulation (EU) No 1094/2010.

Prudential context

1.5 From a prudential perspective, the view of EIOPA is that overall the Solvency II framework is working well.

A risk-based approach to assess and mitigate risks is applied, the insurance industry has better aligned capital to the risks it runs, governance models and their risk management capacity have been significantly strengthened, and insurers throughout Europe use harmonised templates for supervisory reporting, instead of a patchwork of national templates.

1.6 EIOPA's approach to the review overall has therefore been one of evolution rather than revolution. Thus, EIOPA's approach focuses on improving the existing regulation based on the prudential experience during the first years of application and taking into account the changes in the economic context.

In addition, the Commission in its request for advice from EIOPA sought that "the fundamental principles of the Solvency II Directive should not be questioned in the review".

Economic context

1.7 Nonetheless, from the perspective of the economic situation, there are areas of significant concern, which the review should address.

1.8 Subdued economic growth has led to extensive monetary easing and a general flight to safety.

This situation was further intensified by the Covid19 pandemic that has severely affected macroeconomic and market conditions worldwide. In

October 2020, almost the entire euro swap curve moved to negative territory.

1.9 EIOPA's advice is that it is essential to recognise this economic picture in Solvency II.

Since its 2018 review of the Solvency Capital Requirement EIOPA has proposed changes to the treatment of interest rate risk in order to ensure that undertakings hold enough capital for that risk.

In addition, EIOPA recommends changes to the interest rate curves used by insurers to value liabilities, specifically in respect of the extrapolation of those curves.

The changes increase the influence of market interest rates on the extrapolation of the curves, making the liabilities more realistic and improving incentives for risk-management.

1.10 The recognition of the economic picture should reflect two aspects. Firstly, EIOPA's advice potentially sets the regulatory framework for a decade and moreover any implementation of changes resulting from EIOPA's advice is likely to be closer to 2025 than to 2020.

Therefore, EIOPA considers it important that its advice, and its impact, not be unduly influenced by the point in time at which it is written particularly when that point may be atypical.

In light of this EIOPA recommends that the impact of the 2020 review should reflect the economic conditions as at end-2019.

1.11 Secondly, however, the impact of interest rates on insurers is expected to diminish over time reflecting a reduction in liabilities arising from products whose guarantees reflected the era of higher interest rates.

Low interest rates are mainly an issue with regard to the legacy book of insurance contracts.

Those insurance contracts are running off and their relevance for the overall portfolio will reduce over time. EIOPA therefore recommends that its proposal in relation to very low interest rates should likewise reduce over time.

1.12 EIOPA proposes a mechanism intended to reflect these circumstances. Specifically, the proposed new method of extrapolating the risk-free interest rates would have an "emergency brake" which would be applied when interest rate levels were below those of 2019.

The impact of the emergency brake should be temporary and phase out, reflecting the diminishing impact of the legacy book.

The mechanism is calibrated based on EIOPA's advice in all areas which have a material impact on the solvency position of insurers.

The advice on the mechanism should therefore be considered in conjunction with those other areas.

1.13 Regarding investments by insurers, since the introduction of the Solvency II framework the portfolio composition of European insurers has remained broadly stable.

In particular, fixed-income assets dominate the investment portfolios (almost two thirds of the investment portfolio), followed by equities (about 15% of the investment portfolio, including listed and unlisted).

Despite the negative yields experienced, insurers have continued to invest in negative or low yielding bonds. Moreover, this pattern was further strengthened due to flight-to-quality investment behaviour observed during the Covid-19 situation.

1.14 This behaviour is of wider concern in respect of the role of insurers as institutional investors.

Due to their long-term liabilities, life insurance companies in particular are well-suited to long-term investments.

EIOPA's advice is that there can be a more favourable but prudent treatment of insurers' long-term and illiquid liabilities, compared with those of shorter duration, recognising the extent to which such liabilities are predictable and stable.

This is reflected in EIOPA's advice regarding the volatility adjustment.

1.15 More favourable but prudent treatment is recommended for the equities which back long-term and illiquid liabilities.

Equity investments offer higher expected returns than fixed-income markets, but they also carry higher risk reflected in the higher volatility of their returns.

Though some empirical studies suggest that equities are less volatile in the longer-term, the EIOPA analysis did not support the current risk charge.

1.16 Under the Solvency II regulatory framework, the risk of insurers' equity investments is based on one year Value-at-Risk of the portfolio.

This approach reflects that a decrease in the market value of assets leads to a loss of own funds as an insurer could have to sell its assets at any time.

From a prudential perspective, it is important whether during periods of adverse market volatility an insurer is forced to sell its equities or whether it can hold on to them.

Equities which back long-term illiquid liabilities are more capable of being held on to, and therefore a more favourable prudential treatment is justified.

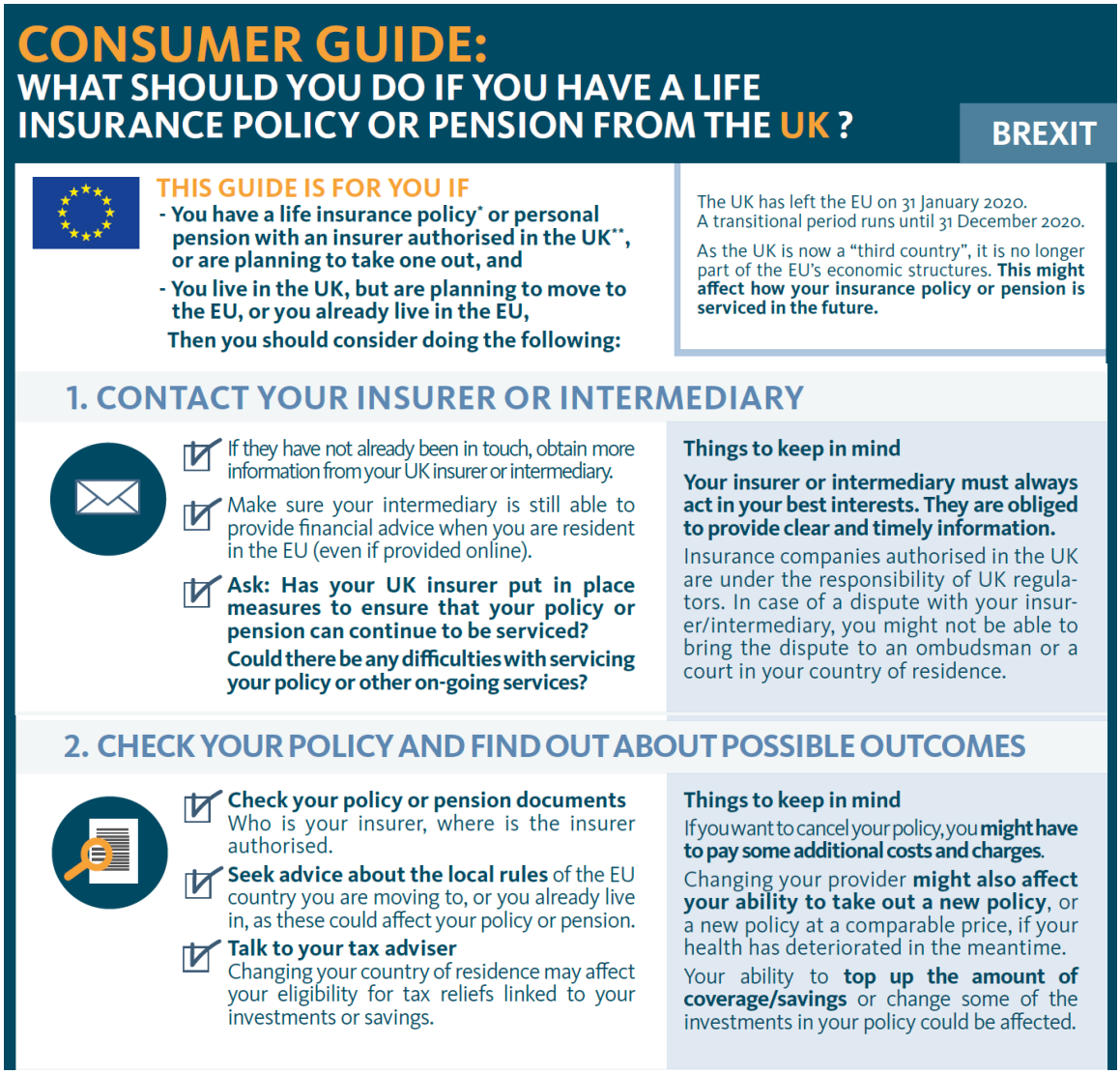
EIOPA's advice focuses on the criteria for the identification of longterm equities which back long-term illiquid liabilities.

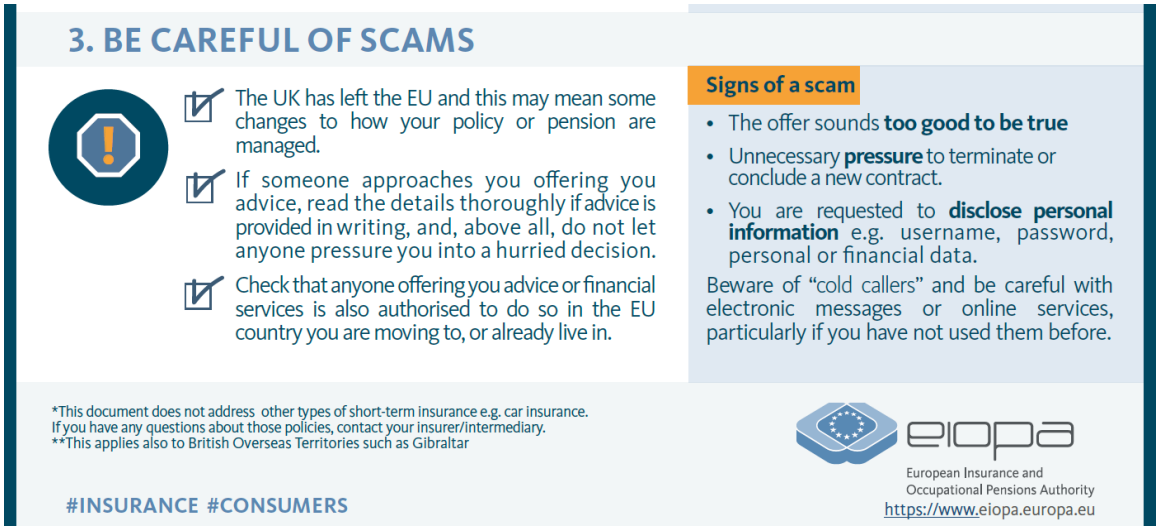
To read more:
https://www.eiopa.europa.eu/sites/default/files/solvency_ii/eiopa-bos-20-749-opinion-2020-review-solvency-ii.pdf

Contents

Consumer guide: What should you do if you have a life insurance policy or pension from the UK?

This consumer guide provides practical information for consumers with a life insurance policy or pension from the UK and living in the European Union or considering moving residence from the UK to the EU.





You may visit:
https://www.eiopa.europa.eu/sites/default/files/publications/consumer_guide_brexit_final.pdf

Guidance issued as SolarWinds compromised

National Cyber Security Centre

SolarWinds, a popular IT system management platform has been compromised and could be used for further attacks on connected systems.

As a result of a cyber attack of their systems, an attacker was able to add a malicious modification to SolarWinds Orion products which allows them to send administrator-level commands to any affected installation.

This modification causes the Orion products to connect to an attacker-controlled server to request instructions and does not rely on the attacker being able to directly connect from the internet to the Orion server.

Not all customers who have an installation with the unauthorised, malicious modification will have been seriously affected, but all should take immediate action.

The NCSC has been working closely with international partners as well as FireEye - a cyber security organisation who discovered the compromise.

In a statement issued earlier this week, we recommended that organisations ensure any affected instances of SolarWinds Orion are installed behind firewalls disabling internet access (both outbound and inbound) for the instances. The statement: https://www.ncsc.gov.uk/news/ncsc-statement-on-fireeye-incident

The NCSC has now also published full guidance highlighting immediate actions for all organisations using the SolarWinds Orion suite of IT management tools. You may visit: https://www.ncsc.gov.uk/guidance/dealing-with-the-solarwinds-orion-compromise

We would also recommend further reading:

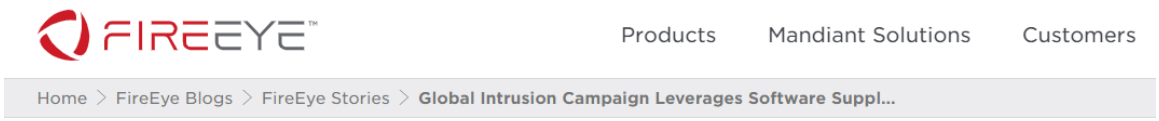
solarwinds

PRODUCTS > SOLUTIONS > SUPPORT > COMMUNITY > FREE TRIALS

SolarWinds Security Advisory

1. SolarWinds have published a security advisory on this incident including details of affected software and the vendor's advice. You may visit: https://www.solarwinds.com/securityadvisory

2. FireEye has published a blog on its investigation. This includes extensive technical details which may help in investigation of a suspected server compromise. You may visit: https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html



FireEye Stories

Global Intrusion Campaign Leverages Software Supply Chain Compromise

3. Microsoft has also published a blog on this attack which includes other potential routes for investigation of compromise. You may visit: https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

ICO statement in response to UK Government's announcement on the extended period for personal data flows, that will allow time to complete the adequacy process

ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Government has announced that the Treaty agreed with the EU will allow personal data to flow freely from the EU (and EEA) to the UK, until adequacy decisions have been adopted, for no more than six months. You may visit: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948093/TCA_SUMMARY_PDF.pdf

This will enable businesses and public bodies across all sectors to continue to freely receive data from the EU (and EEA), including law enforcement agencies.

As a sensible precaution, before and during this period, the ICO recommends that businesses work with EU and EEA organisations who transfer personal data to them, to put in place alternative transfer mechanisms, to safeguard against any interruption to the free flow of EU to UK personal data. You may visit: https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/

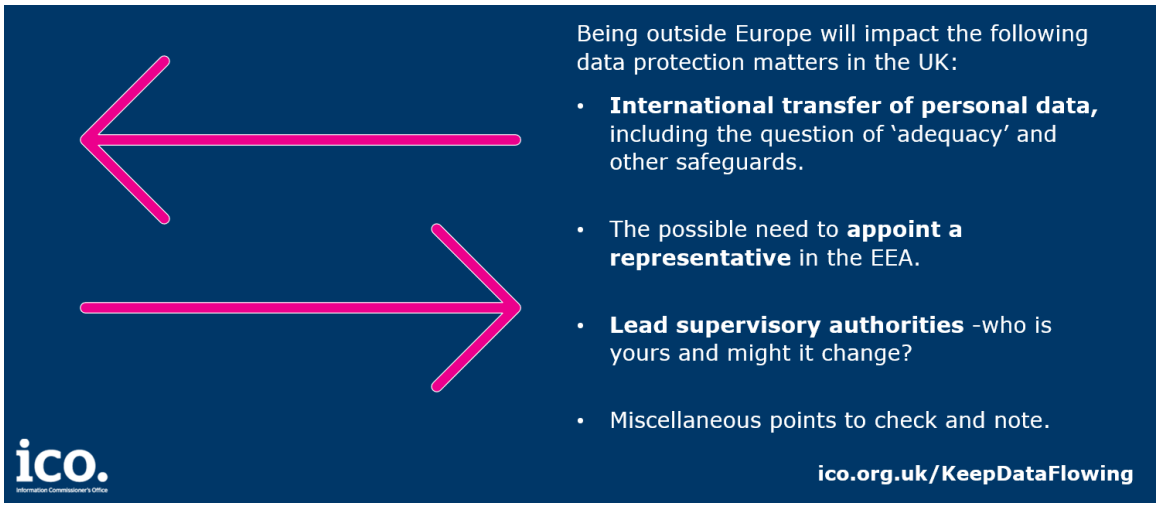
As previously announced, the UK has, on a transitional basis, deemed the EU and EEA EFTA States to be adequate to allow for data flows from the UK.

Information Commissioner, Elizabeth Denham said:

“This is the best possible outcome for UK organisations processing personal data from the EU.”

“This means that organisations can be confident in the free flow of personal data from 1 January, without having to make any changes to their data protection practices.”

“We will be updating the ICO guidance on our website to reflect the extended provisions and ensure businesses know what happens next. At this stage it’s good news for businesses and public bodies.”



MoUs with UK authorities in the area of insurance and pensions

On 5 March 2019, the European Insurance and Occupational Pensions Authority (EIOPA) and all national competent authorities (NCAs) of the European Economic Area (EEA) with competencies in insurance agreed memoranda of understanding (MoUs) with the Bank of England in its capacity as the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) of the United Kingdom (UK).

The MoUs took effect on 1 January 2021, at the end of the transition period following the departure of the UK from the European Union.

The following MoUs were agreed:

- A multilateral MoU on supervisory cooperation, enforcement and information exchange between the EEA NCAs and the UK Authorities.

- A bilateral MoU between EIOPA and the UK Authorities on information exchange and mutual assistance in the field of insurance regulation and supervision.

These MoUs ensure cooperation in the fields of insurance prudential and conduct supervision, for mutual assistance and regular exchange of information.

In addition, EIOPA has agreed a multilateral memorandum of understanding with the Pensions Regulator, which also came into effect on 1 January 2021.

Visit the dedicated webpage for more information related to the UK's departure from the European Union at:
https://www.eiopa.europa.eu/brexit-communication

The financial system after Covid-19

Keynote speech by Mr Benoît Cœuré, Head of the BIS Innovation Hub, at the European Stability Mechanism fourth research seminar of the Regional Financing Arrangements.

Introduction

Distinguished guests, ladies, and gentlemen,

Thank you for inviting me. It is a pleasure to join you virtually today at the fourth research seminar of the Regional Financing Arrangements. And, as a topic, the financial sector landscape post-Covid-19 could not be more timely.

The year 2020 will go down in history as one of the last century's most serious health crises and global economic contractions. The swift response of governments, central banks, and supervisors to mitigate the immediate impact on the real economy has stabilised what could have been catastrophic for global markets.

With mass vaccinations in sight, the policy focus is now shifting from liquidity provision and stabilisation to addressing the long-term scars of the crisis: enabling capital and labour reallocation across industries, and avoiding permanent output losses.

For such reallocation to happen, and to address longerterm sustainability challenges, we need a financial system which is fit for purpose. Could Covid-19 give us the chance to strengthen it?

In my remarks today, I will argue that we first need to draw the lessons of the crisis, and I will focus on two dimensions.

First, there are the known challenges. The reforms after the Great Financial Crisis (GFC) had the effect of pushing risks outside the banking system, as non-bank financial intermediaries (NBFIs) started to fill in the gaps.
We knew it before Covid-19 and the crisis has confirmed it. What does this tell us about the resilience of this new system? Second, there are the unknown challenges.

The crisis has speeded the digitalisation of our economies, accelerating shifts in how companies and individuals work, save and spend. How can technology support the digitalisation of the financial sector post-Covid-19, and can it help regulators make the sector safe and sustainable?

The lessons of Covid-19 for financial sector resilience

Spurred by regulators, banks have built capital and liquidity buffers, improved risk management practices and internalised the social cost of risk-taking. Thanks to these efforts, they were better prepared to cope with a shock in 2020 than they were in 2008.

The jury is still out as to whether all this will suffice to prevent the initial liquidity crisis from morphing into a solvency one. While the scale is unclear at this stage, economic growth and forwardlooking indicators of default risk already suggest that bankruptcies will rise significantly by the end of 2021.

On the other hand, credit spreads are fairly tight, raising concerns about a possible disconnect with fundamentals.

Looking ahead, it will be essential that banks make use of the available capital buffers to absorb losses without excessive deleveraging.

As Carolyn Rogers, the Secretary-General of the Basel Committee on Banking Supervision, recently emphasised, it is too early for banks to take a victory lap over their response to Covid-19.

Holding back on their discretionary distributions of capital makes sense.

Even though the banking sector was not at the epicentre, the turmoil highlighted structural vulnerabilities in the NBFIs sector and the market structures supporting them.

These vulnerabilities have become more important post-GFC, as the footprint of NBFIs has grown – accounting for almost 50% of total financial intermediation globally – and as banks have retreated from certain activities, such as market-making, to preserve balance sheet capacity.

The first weeks of the Covid-1 crisis revealed that the matching and price discovery mechanisms were impaired in large swathes of the capital markets. As conditions worsened, demand soared for cash and near-cash, or short-dated assets. In such circumstances, market liquidity can be as crucial to financial stability as bank solvency or bank liquidity.

As events unfolded, central banks had to intervene to ensure financial stability.

To read more: https://www.bis.org/speeches/sp201217.pdf

Cloud Certification Scheme: Building Trusted Cloud Services Across Europe

ENISA launches a public consultation on a new draft candidate cybersecurity certification scheme in a move to enhance trust in cloud services across Europe.

The European Union Agency for Cybersecurity (ENISA) launched a public consultation, which runs until 7 February 2021, on its draft of the candidate European Union Cybersecurity Certification Scheme on Cloud Services (EUCS).

The scheme aims to further improve the Union's internal market conditions for cloud services by enhancing and streamlining the services' cybersecurity guarantees.

The draft EUCS candidate scheme intends to harmonise the security of cloud services with EU regulations, international standards, industry best practices, as well as with existing certifications in EU Member States.

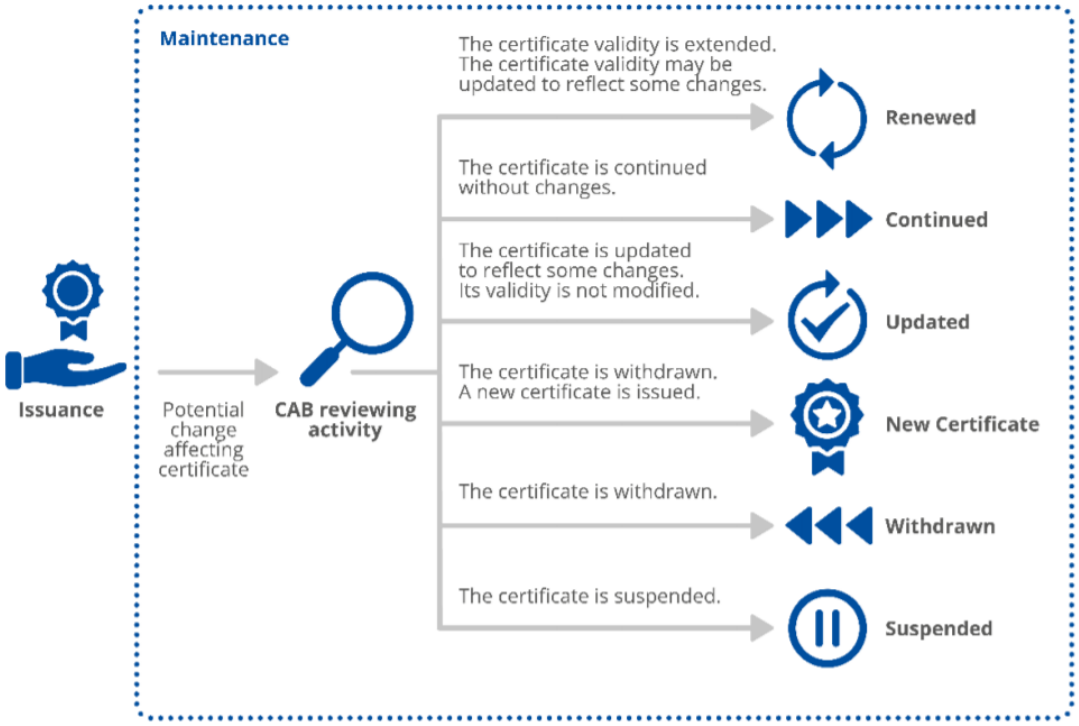
EU Agency for Cybersecurity Executive Director Juhan Lepassaar said: "Cloud services play an increasing role in the life of European citizens and businesses under lockdown; and their security is essential to the functioning of the Digital Single Market. A single European cloud certification is critical for enabling the free flow of data across Europe, and is an important factor in fostering innovation and competitiveness in Europe."

Speaking at the ENISA Cybersecurity Certification Conference on 18 December 2020, Director of Digital Society, Trust and Cybersecurity at the European Commission Directorate-General for Communications Networks, Content and Technology (DG CONNECT) Lorena Boix Alonso said: "We must ensure that cybersecurity certification strikes the right balance, following a sensible risk-based approach, with flexible solutions and certification schemes designed to avoid being outdated quickly. And we need a clear roadmap to allow industry, national authorities and standardisation bodies to prepare in advance."

There are challenges to the certification of cloud services, such as a diverse set of market players, complex systems and a constantly evolving landscape of cloud services, as well as the existence of different schemes in Member States. The draft EUCS candidate scheme tackles these challenges by

calling for cybersecurity best practices across three levels of assurance and by allowing for a transition from current national schemes in the EU.

Figure 2: Processes related to the issuance and maintenance of a certificate



The draft EUCS candidate scheme is a horizontal and technological scheme that intends to provide cybersecurity assurance throughout the cloud supply chain, and form a sound basis for sectoral schemes.

More specifically, the draft EUCS candidate scheme:

- Is a voluntary scheme;
- The scheme's certificates will be applicable across the EU Member States;
- Is applicable for all kinds of cloud services – from infrastructure to applications;
- Boosts trust in cloud services by defining a reference set of security requirements;
- Covers three assurance levels: 'Basic', 'Substantial' and 'High';
- Proposes a new approach inspired by existing national schemes and international standards;
- Defines a transition path from national schemes in the EU;
- Grants a three-year certification that can be renewed;
- Includes transparency requirements such as the location of data processing and storage.

To read more: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/

Climate-related Financial Disclosures (TCFD)

FSB encourages the IFRS Foundation and authorities to use TCFD's recommendations as the basis for climate-related financial risk disclosures

Globally consistent and comparable disclosures by companies of their climate-related financial risks are increasingly important to market participants and financial authorities as a means to give financial markets the information they need to manage risks, and seize opportunities, stemming from climate change.

The FSB created the Task Force on *Climate-related Financial Disclosures (TCFD)* in 2015 to develop a set of voluntary disclosure recommendations for use by companies in providing decision-useful information to investors, lenders and insurance underwriters about the climate-related financial risks that companies face.

The TCFD published its disclosure recommendations in 2017.

Since then, nearly 1,700 organisations have expressed their support for the TCFD recommendations.

Nearly 60% of the world's 100 largest public companies support the TCFD, report in line with the TCFD recommendations, or both.

The TCFD continues to promote and monitor adoption of its recommendations worldwide and issued supplementary guidance to support implementation.

Alongside this industry-led progress in promoting consistent voluntary climate-related disclosures, a growing number of official sector initiatives are developing requirements or guidance at the national or regional level, or considering the development of international standards.

It is important that steps by the official sector and private sector are well aligned in promoting globally consistent disclosures and avoiding fragmentation.

The FSB therefore welcomes the recommended approach by the Trustees of the IFRS Foundation to initially focus on standards for climate-related financial disclosures, as set out in the September 2020 IFRS Consultation Paper on Sustainability Reporting.

The initial focus on climate-related information would be appropriate given the growing interest of investors in the topic for financial risk management and the importance of global consistency in the actions that are already beginning to be taken by national and regional authorities to develop requirements and guidance in this area.

Such internationally agreed minimum standards for disclosures would, as usual, not preclude individual authorities from going further if they wish.

The FSB strongly encourages the IFRS Foundation to build on the work of the TCFD, by using the TCFD's recommendations as the basis for standards for climate-related financial disclosures.

The TCFD recommendations set out a comprehensive framework that has been developed by, and is directly responsive to the needs of, users and preparers of financial filings across a range of financial and non-financial sectors around the world.

The TCFD's recommendations have attracted widespread support from users and preparers.

The FSB strongly encourages national or regional authorities that are developing requirements or guidance for climate-related disclosures to consider using the TCFD recommendations as the basis.

Such consistency in approach would help to avoid the risk of market fragmentation, both across jurisdictions, and between requirements and guidance being developed today and international standards that may be introduced in the future.

To further promote global coordination, the FSB will explore with standard-setters and other international bodies ways to promote globally comparable, high-quality and auditable standards of disclosure based on the TCFD recommendations.

The FSB will report to the G20 Finance Ministers and Central Bank Governors meeting on progress in this area in July 2021.

Financial Stability Oversight Council (FSOC), Annual Report

The U.S. economy was in the midst of the longest post-war economic expansion, with historically low levels of unemployment, prior to the onset of the COVID-19 pandemic earlier this year.

The global pandemic not only brought about a public health crisis but also caused a contraction of economic activity at an unprecedented pace.

Initially, the pandemic reduced consumer spending, slowed manufacturing production, and led to widespread business closures.

The unemployment rate surged from 3.5 percent in February to a record high of nearly 15 percent in April.

Since then, extraordinary measures undertaken by policymakers have succeeded in arresting the decline in economic conditions, initiating a recovery and lowering the unemployment rate to 7.9 percent as of September.

However, a protracted virus outbreak poses downside risks that can slow the recovery and even prolong the economic downturn.

Financial Stress from the COVID-19 Pandemic and the Policy Response

The COVID-19 outbreak led to substantial financial stress in the first quarter of 2020.

While economic activity was disrupted in March, investors fled riskier assets for the safety and liquidity of cash and shortterm government securities.

A broad-based selloff in equities and commodities resulted in sharp declines in both spot and futures prices.

The sectors most affected by the pandemic, such as airlines, energy, transportation, hotels, and restaurants, recorded the sharpest declines.

The flight to safety and liquidity also created disruptions in short-term and global dollar funding markets.

Meanwhile, trading conditions for Treasuries and agency mortgagebacked securities (MBS), generally considered safe and liquid assets, were also strained.

Moreover, credit conditions tightened in the commercial paper (CP), corporate bond, and municipal debt markets.

With the stress in funding markets in March, precautionary draws by nonfinancial businesses on existing lines of credit with banks increased sharply, as firms tried to cover shortfalls in revenues and reductions in the availability of short-term funding.

Substantially increased liquidity and capital requirements imposed after the 2008 financial crisis helped banks meet the large, unanticipated drawdowns.

Large deposit inflows from investors fleeing to the safety of deposit insurance and borrowings at the Federal Reserve's discount window also helped in meeting this surge in liquidity demand.

Meanwhile, policymakers acted to minimize the health and economic effects of the pandemic.

On March 27, the Coronavirus Aid, Relief, and Economic Security (CARES) Act was signed into law.

The CARES Act authorized approximately $2.6 trillion in funding to address COVID-19 and to support the economy, households, businesses, and other entities.

In addition, the Federal Reserve and Treasury undertook a series of extraordinary measures beginning in March to contain the financial fallout from the pandemic.

The Federal Reserve also lowered the target federal funds rate to near zero and substantially increased purchases of Treasuries and agency MBS to ease trading pressures.

In a bid to stabilize short-term funding markets (STFMs), the Federal Reserve launched a series of facilities to provide liquidity to foreign central banks, primary dealers, depository institutions, and money market funds.

In light of these exigent circumstances, the Federal Reserve and Treasury also enacted a series of unprecedented measures to support corporate bonds, bank loans, longer-term municipal debt, and asset-backed securities.

These credit and lending facilities were developed with the goal of relieving strains in longer-term debt markets through the pandemic. These policy actions have substantially improved market conditions and investor sentiment in financial markets.

Federal Reserve purchases of Treasuries and agency MBS reduced bid-ask spreads and relieved the stress in trading conditions for these securities.

The announcement of liquidity facilities not only succeeded in lowering spreads on CP and short-term municipal securities but also reversed the heavy redemptions from prime and tax-exempt money funds. The creation of new credit facilities lowered spreads on corporate bonds and revived new issuance in both the investment grade and high-yield bond segments.

Overall, these policy measures have restored the orderly functioning of financial markets and improved investor sentiment, as reflected in the rebound in corporate financing and equity prices.

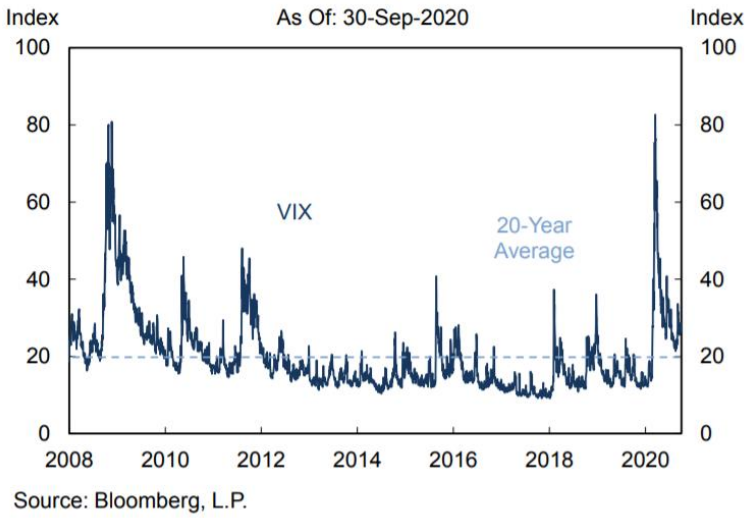
The Council provided an important venue for facilitating coordination and analysis of risks across member agencies at the onset of the pandemic and throughout the year.

Council members regularly identified key risks and shared information regarding their policy responses. The Council also increased the frequency of staff-level meetings to allow important analyses of major market developments to be shared in a timely manner with all Council member agencies.

In addition, the Council's previous identification of vulnerabilities and analysis that it had performed leading up to the financial stress helped ensure that policymakers' responses were more coordinated, well informed, and effective.

The report (216 pages):
https://home.treasury.gov/system/files/261/FSOC2020AnnualReport.pdf

3.2.2.1 S&P 500 Volatility



Source: Bloomberg, L.P.

The Cybersecurity Strategy

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy.

The aim of this strategy is to bolster Europe's collective resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

This includes the ever-increasing number of connected and automated objects in our homes, offices and factories.

The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses.

The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources both inside and outside the EU.

The EU should therefore be leading the efforts for a secure digitalisation.

It should be driving norms for world-class solutions and standards of cybersecurity for essential services and critical infrastructures, as well as driving the development and application of new technologies.

Governments, businesses and citizens will all share a responsibility in ensuring a cyber-secure digital transformation.

What is the strategy about?

The strategy describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign.

It also lays out how the EU can step up its cooperation with partners around the world who share our values of democracy, rule of law and human rights.

This technological sovereignty needs to be founded on the resilience of all connected services and products.

All the four cybercommunities – those concerned with the internal market, with law enforcement, diplomacy and defence – need to work more closely towards a shared awareness of threats.

They should be ready to respond collectively when an attack materializes, so that the EU can be greater than the sum of its parts.

The strategy covers the security of essential services such as hospitals, energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories.

The strategy aims to build collective capabilities to respond to major cyberattacks. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace.

Moreover, it outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to Member States and the EU.

Main aim of the strategy

The new strategy aims to ensure a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe.

Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments.

These three instruments are regulatory, investment and policy initiatives.

They will address three areas of EU action:

- resilience, technological sovereignty and leadership;
- operational capacity to prevent, deter and respond;
- cooperation to advance a global and open cyberspace.

The EU is committed to supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years. This would quadruple previous levels of investment.

It demonstrates the EU’s commitment to its new technological and industrial policy and the recovery agenda. The EU’s new Cybersecurity Strategy for the Digital Decade forms a key component of Shaping Europe’s Digital Future, the Commission’s Recovery Plan for Europe and of the Security Union Strategy 2020-2025.

You may visit: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

https://ec.europa.eu/info/strategy/recovery-plan-europe_en

https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

Response to COVID-19 and medium- to long-term challenges for Japan's economy - with an eye on the post-COVID-19 era

Haruhiko Kuroda, Governor of the Bank of Japan, at the meeting of Councillors of Nippon Keidanren (Japan Business Federation), Tokyo.

Introduction

It is a great honor to have this opportunity to address such a distinguished gathering of business leaders in Japan today.

For eight years now, I have delivered a speech at this end-of-year meeting, and I can say that this year we have experienced enormous changes in the social and economic environment due to the shock of the novel coronavirus (COVID-19).

As we wrap up 2020, I would first like to take a look back at economic developments this year, mainly focusing on the impact of COVID-19, and talk about the outlook for economic activity and prices.

Then, I will explain the Bank of Japan's thinking behind its policy responses.

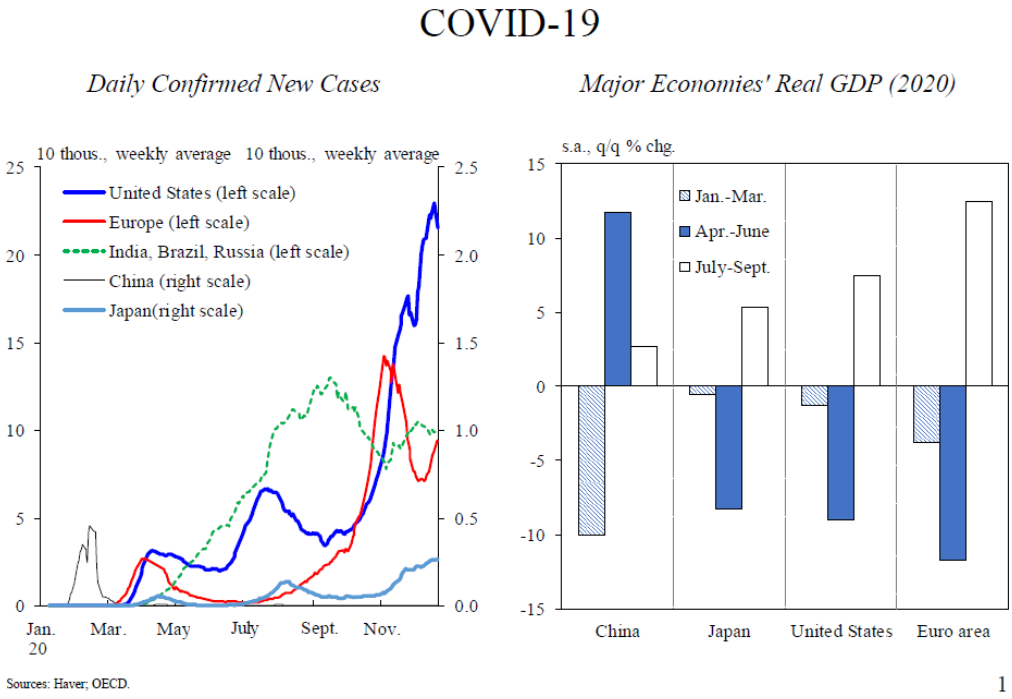
In relation to the conduct of monetary policy, I will also touch on the conduct of the assessment for further effective and sustainable monetary easing, which the Bank decided at the Monetary Policy Meeting (MPM) held last week.

Lastly, I would like to talk about what is necessary in taking advantage of lessons to be learned from overcoming the current crisis for future growth -- that is, challenges regarding Japan's economy as a whole that should be addressed when also looking ahead to the post-COVID-19 era from a medium- to long-term perspective.

I. Economic and Price Developments during the COVID-19 Era and Their Outlook Impact of COVID-19 on the Economy

I. Economic and Price Developments during the COVID-19 Era and Their Outlook

Chart 1



Let me start with a look back at economic developments this year, mainly focusing on the impact of COVID-19.

COVID-19 started to spread from the beginning of the year and became a pandemic within a short period toward early spring (Chart 1).

Governments around the world took strict and wide-ranging public health measures in order to prevent the spread.

Under these circumstances, the global economy became depressed significantly.

However, since the summer season, as public health measures have been eased, the global economy has picked up from that state of significant depression, as seen in the growth rates of each country turning positive on a quarter-on-quarter basis.

Similar developments have been observed in Japan.

The quarter-on-quarter GDP growth rate for the April-June quarter registered a considerably negative figure of minus 8.3 percent with wide-ranging economic activities being constrained.

However, that for the July-September quarter turned positive, to 5.3 percent, and Japan's economy has picked up from the bottom, although it has remained in a severe situation.

The economic fluctuation this time is different in nature from what was seen in the past.

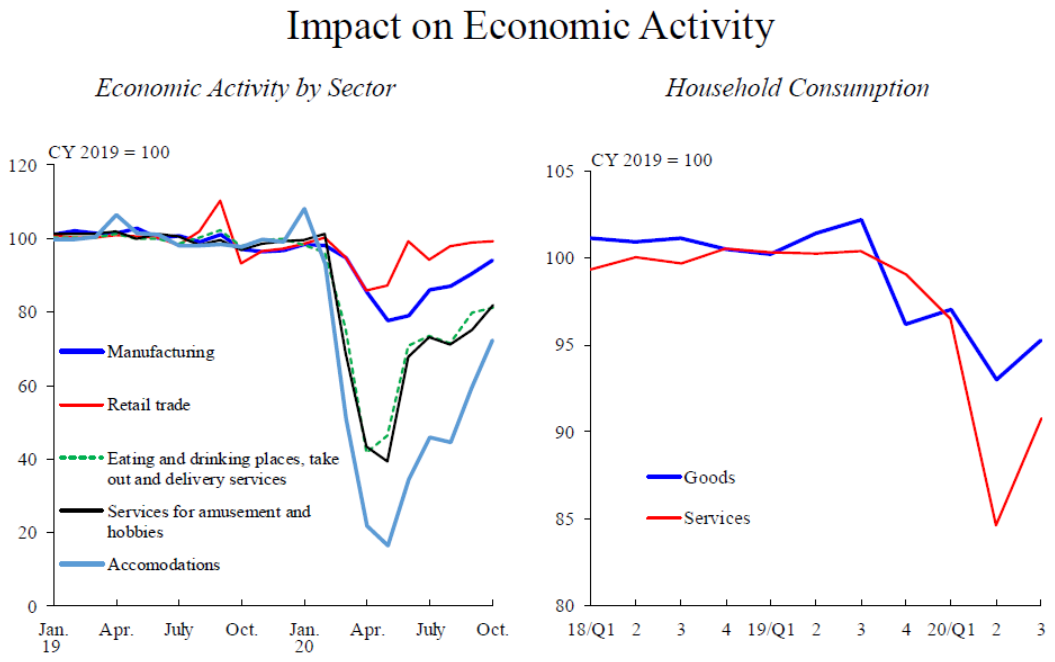
Most of the fluctuations since World War II were triggered by cyclical adjustments in business fixed investment and in inventory investment, or by financial imbalances.

On the other hand, the current fluctuation is exceptional, in that it stemmed from a shock caused by an infectious disease, which is not inherent in the economy, and that economic activity has been constrained exogenously with a view to preventing the spread of the disease.

In other words, such activity has been affected largely by an epidemiologic factor.

I. Economic and Price Developments during the COVID-19 Era and Their Outlook

Chart 2



Note: In the left-hand chart, figures for manufacturing are the "Indices of Industrial Production" and those for other sectors are the "Indices of Tertiary Industry Activity."
Sources: Ministry of Economy, Trade and Industry; Cabinet Office.

2

Reflecting the characteristics of COVID-19, economic activities that involve social interaction are particularly affected, and this is another point that is unique to the current case (Chart 2).

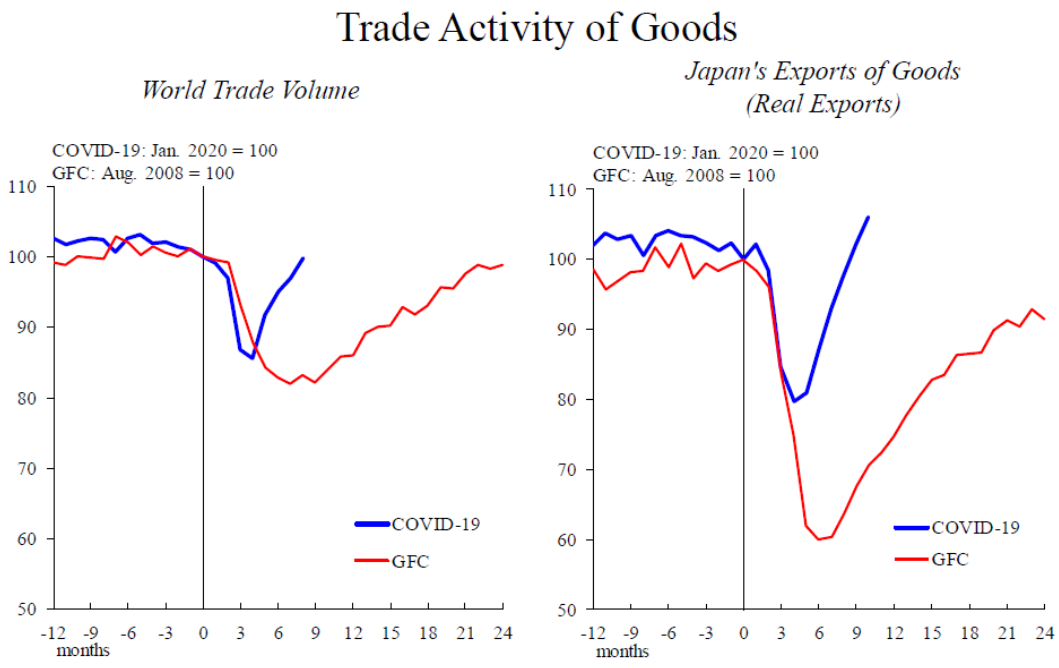
Looking at economic activities of firms in Japan by sector, a significant decline has been seen in the industry of face-to-face services such as eating

and drinking as well as accommodations -- where firms are relatively small -- and amusement services including events.

In terms of household spending, consumption of services has declined considerably compared with that of goods. A constraint on services consumption is due to vigilance against COVID-19, and the differences in consumption behavior of each age group reflect the degree of their vigilance.

That is, services consumption by the younger generation has recovered rapidly, whereas that by seniors, who are strongly vigilant against COVID-19, saw a significant decline and has picked up at a slower pace. In contrast, manufacturing and retail firms, which produce and sell goods, have been relatively less affected.

Chart 3



Sources: CPB Netherlands Bureau for Economic Policy Analysis; Bank of Japan; Ministry of Finance.

3

Goods transactions worldwide have picked up at a comparatively faster pace (Chart 3).

A decline in global trade activity has been small compared with at the time of Global Financial Crisis (GFC) and a rapid recovery has been observed. Under these circumstances, the level of Japan's exports has returned to that seen prior to the COVID-19 outbreak, and at a rapid pace. This has led to manufacturers' relatively steady production activity.

As I have explained thus far, the impact of the shock of COVID-19 is uneven and largely varies for attributes such as the industry and size of firms as well as consumers' ages.

At the current phase in particular, this suggests the need to closely examine economic developments not only by looking at the aggregate or average values of data, but also through analyzing developments in different attributes of each economic entity.

To read more: https://www.bis.org/review/r201228a.pdf

Covid-19 and cyber risk in the financial sector

Bank for International Settlements, Iñaki Aldasoro, Jon Frost, Leonardo Gambacorta, David Whyte

Key takeaways

• The financial sector has been hit by hackers relatively more often than other sectors during the Covid19 pandemic.

• While this has not yet led to significant disruptions or a systemic impact, there are substantial risks from cyber attacks for financial institutions, their staff and their customers going forward.

• Financial authorities are working to mitigate cyber risks, including through international cooperation.

During the Covid-19 pandemic, financial institutions have been at the leading edge of the response to cyber risk.

Their already large exposure to cyber risk has been further accentuated by the move towards more working from home (WFH) and other operational challenges.

This Bulletin serves as a primer on cyber risk and presents initial findings on how the financial sector has met the challenges of the pandemic.

We draw on new data to assess changes in the threat landscape for financial institutions in the pandemic.

Cyber risk: a taxonomy

As the economy and financial system become more digitised, cyber risk is growing in importance.

"Cyber risk" is an umbrella term encompassing a wide range of risks resulting from the failure or breach of IT systems.

According to the FSB Cyber Lexicon (2019), cyber risk refers to "the combination of the probability of cyber incidents occurring and their impact".

A "cyber incident", in turn, is "any observable occurrence in an information system that:

(i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or

(ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not".

Cyber risk is one form of operational risk (Aldasoro et al (2020b), CPMI-IOSCO (2016)).

Cyber risks can be classified based on their cause/method, actor, intent and consequence (Aldasoro et al (2020a), Curti et al (2019)).

The causes or methods vary, and include both unintended incidents and intentional attacks.

Examples of the former are accidental data disclosure, and implementation, configuration and processing errors.

Such incidents are frequent. Yet around 40% of cyber incidents are intentional and malicious, rather than accidental, ie they are cyber attacks (Aldasoro et al (2020c)).

Some cyber attacks involve threat actors inserting themselves into a trusted data exchange.

Malware (ie "malicious software") is software designed to cause damage to IT devices and/or steal data (for example, so-called Trojans, spyware and ransomware).

Man-in-the-middle attacks occur when attackers insert themselves into a two-party transaction (Graph 1, first panel), accessing or manipulating data or transactions.

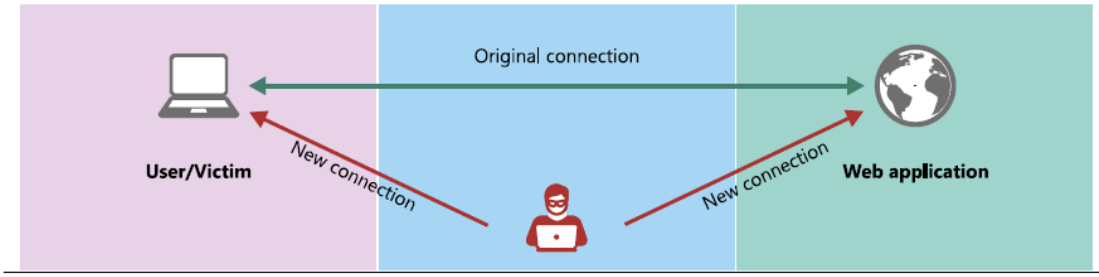
Cross-site scripting is a web security vulnerability that allows attackers to compromise the interactions a victim has with a vulnerable application. Phishing is stealing sensitive data or installing malware with fraudulent emails that appear to be from a trustworthy source (Graph 1, second panel).

To gain a victim's trust, phishing attacks may imitate trusted senders.

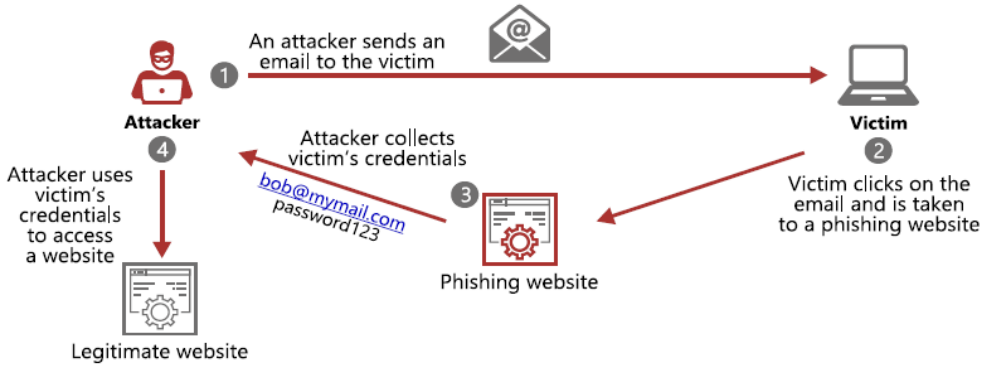
After gaining entrance, these may help attackers to gain credentials and entry into a system.

Selected causes of cyber attacks — Graph 1

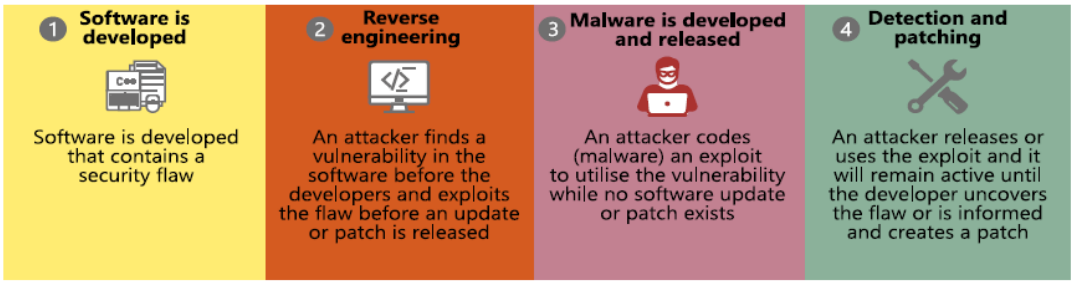
Man-in-the-middle



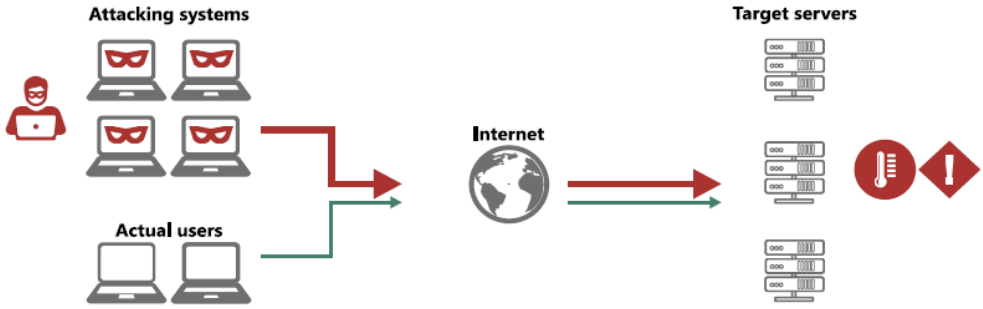
Phishing



Timeline of zero-day vulnerabilities



Distributed denial-of-service (DDoS) attack

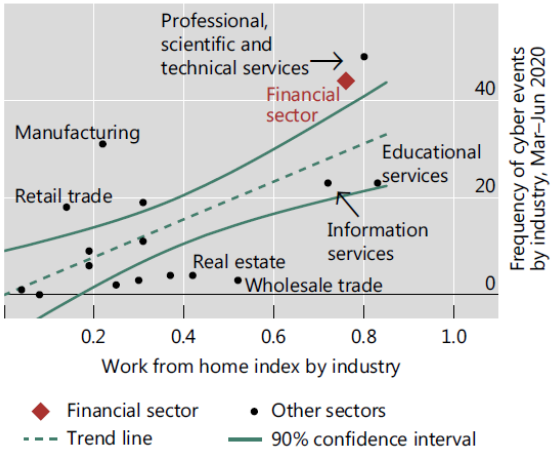


Source: Authors' elaboration.

Password cracking is the process of recovering secret passwords stored in a computer system or transmitted over a network.

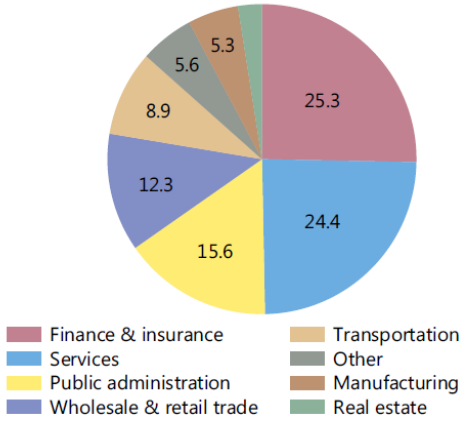
The financial sector has been hit by cyber attacks during the pandemic — Graph 2

WFH index versus cyber events during Covid-19[1]



Covid-19-related cyber events by sector[2]

Per cent



[1] Excludes the health sector. [2] Based on cases classified by Advisen as Covid-19-related. Includes data up to 9 September 2020. The sample in the graph excludes the health sector (57 Covid-related cases) and affecting health-related items of the manufacturing sector (163 cases).

Sources: Dingel and Neiman (2020); Advisen; authors' calculations.

To read more: https://www.bis.org/publ/bisbull37.pdf

Cyberattack on EMA

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Update 1

The full investigation launched by the European Medicines Agency (EMA), in close cooperation with law enforcement and other relevant entities, demonstrated that data has been breached. An initial review revealed that a limited number of documents belonging to third parties were unlawfully accessed. The concerned companies are being informed.

The Agency remains fully functional and its timelines related to the evaluation and approval of COVID-19 vaccines and treatments are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigations.

Update 2

EMA has engaged a specialised third-party service provider to support the full investigation that is currently being carried out in close cooperation with law enforcement and other relevant entities. This company will contribute to the additional security measures that are being put in place in response to the data breach.

So far, the investigation has revealed that a limited number of documents belonging to third parties were unlawfully accessed. The concerned third parties identified at this stage have been contacted and duly informed.

The Agency remains fully functional and its timelines related to the evaluation and approval of COVID-19 vaccines and treatments are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigations.

Update 3

The ongoing investigation of the cyberattack on EMA, carried out by the Agency in close collaboration with law enforcement and other relevant entities, has revealed that the data breach was limited to one IT application. The perpetrators primarily targeted data related to COVID-19 medicines and vaccines and unlawfully accessed documents belonging to third parties. The companies concerned at this stage have been contacted and duly informed.

As the investigation proceeds, and all potentially suspicious activity is analysed, the Agency will ensure that any additional third party whose documents may have been subject to unauthorised access is notified.

The Agency and the European medicines regulatory network remain fully functional and timelines related to the evaluation and approval of COVID-19 medicines and vaccines are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigation.

Update 4

The ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines belonging to third parties have been leaked on the internet. Necessary action is being taken by the law enforcement authorities.

The Agency continues to fully support the criminal investigation into the data breach and to notify any additional entities and individuals whose documents and personal data may have been subject to unauthorised access.

The Agency and the European medicines regulatory network remain fully functional and timelines related to the evaluation and approval of COVID-19 medicines and vaccines are not affected.

EMA will continue to provide information in due course, to the extent possible, given its duty towards the ongoing investigation.

You may visit: https://www.ema.europa.eu/en/news/cyberattack-ema-update-4

Reviving and Restructuring the Corporate Sector Post-Covid

The coronavirus pandemic, by dramatically changing consumption patterns and business operations, is triggering a major corporate solvency crisis in many countries.

Apart from policies directly supporting employment, initial policy responses to support businesses focused heavily on liquidity issues. Some liquidity support is still needed, but the crucial issue now is solvency.

Policymakers need to act urgently, as the solvency crisis is already eroding the underlying strength of the business sector in many countries.

The problem is worse than it appears on the surface, as massive liquidity support, and the confusion caused by the unprecedented nature of this crisis, are masking the full extent of the problem, with a “cliff edge” of insolvencies coming in many sectors and jurisdictions as support programs lose funding and existing net worth is eaten up by losses.

However, the difficulty of predicting the duration and recovery path after the pandemic, and of differentiating between structural versus temporary changes in demand, makes it hard to determine the long-term viability of enterprises during the pandemic.

This complicates the targeting and design of measures to support the corporate sector.

This solvency crisis differs sharply from the global financial crisis, which centered on the financial system and on liquidity problems.

Some of the answers from that previous crisis are valid now, but new approaches are also needed.

The first wave of liquidity-focused policy measures has prevented much more severe consequences for the corporate sector, jobs, and for the economy more broadly.

As the crisis progresses, jurisdictions now need to develop policy responses that accommodate structural changes in the economy triggered by the pandemic, and address the following problems that make the initial response unsustainable:

• Inadequate targeting of support, which fails to sufficiently tailor the policy response to the situations of different firms

• An excessive focus on credit provision, which risks overburdening firms with debt, promoting inefficient use of resources, and engendering future problems

• Excessive direct government decision-making and suboptimal use of private sector expertise that could be used to better direct support

• A level of public spending that would be unsustainable over the potential duration of the ongoing economic crisis.

In this report we recommend for policymakers:

• A set of universal core principles to guide the design of the policy response

• A set of potential tools with which to respond

• A decision framework to determine appropriate policy responses for a specific jurisdiction.

To read more:
https://group30.org/images/uploads/publications/G30_Reviving_and_Restructuring_the_Corporate_Sector_Post-Covid.pdf

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Solvency II Association

At every stage of your career, our association provides networking, training, certification, information, updates, alerts, and services you can use. Join us. Stay current. Take advantage of the new opportunities. Read our monthly newsletter. Get certified.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit: https://www.solvency-ii-association.com/How_to_become_member.htm

2. Monthly Updates – Visit the Reading Room of the association at: https://www.solvency-ii-association.com/Reading_Room.htm

3. Training and Certification – You may visit: https://www.solvency-ii-association.com/CSiiP_Distance_Learning_Online_Certification_Program.htm

For instructor-led training, you may contact us. We tailor Solvency II presentations, awareness and training programs for supervisors, boards of directors, employees, service providers and consultants.