International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.iambd.org

News for the Board of Directors, June 2022

Dear members and friends,

Henry Ohlsson, Deputy Governor of Sveriges Riksbank, gave an interesting presentation at the Uppsala University:

Monetary policy and inflation in times of war

The 2020s could certainly have begun better. Following a pandemic, which we still haven't quite seen the end of, another war has broken out in Europe.

As information now spreads faster than ever before, via news channels and social media, and as it is a country quite close to us that has been affected, the war in Ukraine has shaken us more than usual in our safe Swedish everyday lives. That, at least, is how I feel.

However horrific the war in Ukraine may be, it is not the war as such that I intended to talk about today, but its economic consequences – and those of war in general.

After all, it is in the field of economics that I have my comparative advantages, and as policy-maker at a central bank, monitoring the economic consequences is, of course, something that is part of my job. I will focus on the effects on inflation, as they are particularly important for a central bank.

When major and unusual events such as a war occur, there is no 'manual' for how to act as an economic policy decision-maker.

All wars are different – in terms of their scale and duration, their location and their impact on the world around them. Instead, we must brush up on our possible knowledge of history and try to see if there are past historical episodes from which we can learn something for the current situation.

It is of course also important to study the available literature on the economic consequences of war to see whether it is possible to find common denominators that can give clues regarding the situation that has arisen.

What I intend to do today is to first briefly review what research literature has to say about the connection between war and inflation. Then I will look back at previous episodes when war was associated with rising inflation in Sweden and draw some conclusions from this.

Finally, I intend to say something about how I view the current situation from a monetary policy perspective. As usual, it is my personal views that I am expressing.

War often leads to inflation

The fact that war and inflation often go hand in hand has been known for a very long time. Back in 500 BC Sun Tzu, Chinese general and author of a book on the art of war, observed: "Where the army is, prices are high; when prices rise the wealth of the people is exhausted."

What this refers to is, of course, that an army of perhaps tens of thousands of soldiers requires a lot of resources just to stay alive and these can be difficult to raise in a geographically restricted area.

Demand simply rises in relation to the available supply of food and other necessities, and this causes inflation to rise. If, as has often been the case throughout history, the army supports itself by looting, it may be able to survive for a while, but for the civilian population, prices will rise because supply decreases.

Of course, an army could not survive indefinitely in one place, because resources sooner or later run out. In his book “Ofredsår” (“Years of Trouble”), Peter Englund has likened the Swedish army during the Thirty Years’ War to a shark that must be constantly on the move to avoid succumbing.

Once a war had started, the armies of the time lived partly their own lives, separated from the state, and largely organised their own supplies, especially of course during campaigns abroad. Inflation therefore increased more locally depending on where the armies happened to be, as a result of the demand for food and other necessities exceeding supply.

Rising demand and printing money

When a country rearms and fights a war, inflation can also rise in the whole economy for the same reason, that is, demand rises in relation to supply.

A sharp increase in public expenditure as a result of rearmament or war effort increases capacity utilisation in the economy and can therefore lead to higher inflation.

In connection with the Second World War, the US economy approached full capacity utilisation, which contributed to a rise in inflation. Some economists argue that it was the US rearmament in connection with the war that finally put an end to the 1930s depression.

The way in which a rearmament or war is financed is also of great importance to the way in which inflation develops. The financing can entail increasing taxes or decreasing expenditures other than military, by raising loans or by making the central bank print more money. If a war is financed by increasing taxes or decreasing other expenditure, public purchasing power will be reduced.

This counteracts the inflationary effect of increased public expenditure. At the same time, tax financing may be politically difficult to implement. In the short term, the politically easiest way of financing war, but in the longer term perhaps the most harmful, is through the printing of money, as this almost inevitably results in higher inflation.

A fairly large share of the literature on the effects of war on inflation is about the financing of war. A review of the effects on inflation of the United States’ wars from the American Revolution to the First Gulf War shows that when the US has been involved in more limited wars, they have usually been financed through higher taxes or increased borrowing or a combination of these.

However, in the case of major wars, the point where these two methods of financing have been considered exhausted has often been reached, and the government therefore turned to the printing press. The result has often been a considerably higher inflation rate.

The two world wars are examples of this. After a war, sovereign debt has often increased considerably. At the same time, it may be difficult to raise tax revenue in the same way as before the war.

This may be because the political situation has become more unstable or the economy's production capacity has declined. In such a situation, there may be a great temptation for a government to try to alleviate the situation by using the printing press to finance current expenditure and pay off the loans.

Difficulties in generating sufficient tax revenues are considered to be an important explanation for the high inflation in countries such as Germany, Austria, Hungary, Poland and Russia after the First World War and also for the highest rate of hyperinflation in the modern age, that in Hungary in 1945- 1946. According to some estimates, prices at their fastest then doubled in fifteen hours.

To read more:
https://www.riksbank.se/globalassets/media/tal/engelska/ohlsson/2022/ohlsson---monetary-policy-and-inflation-in-times-of-war.pdf

Bank of England publishes results of the 2021 Biennial Exploratory Scenario: Financial risks from climate change

Bank of England

The Bank of England (the Bank) has run its first exploratory scenario exercise on climate risk, involving the largest UK banks and insurers.

This exercise supports the Financial Policy Committee (FPC) and Prudential Regulation Committee (PRC) in the pursuit of their statutory objectives. The financial risks from the physical effects of climate change and the transition to a net-zero economy have the potential to affect the vulnerability of banks and insurers to shocks, and the stability of the wider financial system.

The Prudential Regulation Authority's (PRA's) primary objectives are to promote the safety and soundness of firms that it regulates, and to contribute to the protection of insurance policyholders.

The FPC's primary objective is to protect and enhance the stability of the financial system of the United Kingdom. The FPC also has a secondary objective to support the economic policy of Her Majesty's Government, which includes ensuring the financial system can support the transition to a net-zero economy.

The Climate Biennial Exploratory Scenario (CBES) includes three scenarios exploring both transition and physical risks, to different degrees.

The exercise considered two possible routes to net-zero UK greenhouse gas emissions by 2050: an 'Early Action' (EA) scenario and a 'Late Action' (LA) scenario. A third 'No Additional Action' (NAA) scenario explores the physical risks that would begin to materialise if governments around the world fail to enact policy responses to global warming.

The CBES scenarios are not forecasts of the most likely future outcomes. Instead, they are plausible representations of what might happen based on different future paths of climate policies, technological developments and consumer behaviour, aimed at limiting the rise in global temperatures. Each scenario is assumed to take place over a period of 30 years.

In line with the stated aims of the exercise, the CBES has:

1. Assisted participants in enhancing their management of climate-related financial risks (hereafter 'climate risks'), including by fostering engagement with their large corporate customers to understand their vulnerability to climate risks.

The CBES has shown that UK banks and insurers are making good progress in some aspects of their climate risk management, and this exercise has spurred on their efforts further. But the Bank's assessment is that UK banks and insurers still need to do much more to understand and manage their exposure to climate risks.

The lack of available data on corporates' current emissions and future transition plans is a collective issue affecting all participating firms. The Bank will give firm-specific feedback to participants, and will use findings from the CBES to help target their efforts.

2. Sized the financial exposures of participants to climate risks.
Climate risks captured in the CBES are likely to create a drag on the profitability of banks and insurers, particularly if they are unable to manage these risks effectively.

But there is substantial uncertainty around the true magnitude of these risks. And climate risks outside the scope of the CBES (such as trading losses for banks and mortality risk for life insurers) could be material.

3. Allowed policy makers to gauge challenges to banks' and insurers' business models from climate risk, to understand their likely responses, and to analyse the implications of those responses for the system as a whole.

All participating banks and insurers have published climate strategies or net-zero transition plans, which they broadly followed in their responses to all three of the CBES scenarios. Individual plans involve reducing finance, and in some cases insurance, to the most carbon-intensive industries, as well as engaging with corporate clients and counterparties to help facilitate their transition to net zero.

There is a risk, however, that the collective impact of such plans could have negative consequences for the wider economy. For example, there could be economic consequences if limits on lending and insurance to corporates involved in the supply of more carbon-intensive energy run ahead of the expansion of renewable energy supply and other measures to improve energy efficiency.

A transition to net zero would materially impact a number of sectors that banks and insurers are exposed to, forcing those in such sectors to adapt their business models or potentially risk becoming unviable over time.

It will be in banks' and insurers' collective interests both to support the adaptation of those counterparties across the economy that have credible transition plans, and to gradually reduce their exposures to sectors of the economy that become less economically viable as a result of the transition

to net zero. Banks and insurers noted that they will be better able to prepare and plan for the transition if the evolution of climate policy is clear and well communicated.

Some responses – to the NAA scenario in particular – implied a material reduction in access to lending and insurance for sectors and households which were most exposed to physical risks.

In the NAA scenario, banks would reduce lending to properties facing greater physical risks, and insurers would substantially increase the premiums they charge to insure against such risks, making insurance coverage unaffordable for many of these households.

Key lessons and next steps

One recurrent theme across participants' submissions was a lack of data on many key factors that participants need to understand to manage climate risks. Another was the range in the quality of different approaches taken across organisations to the assessment and modelling of these risks.

All participating firms have more work to do to improve their climate risk management capabilities. The Bank will engage with firms individually and collectively to help them target their efforts, and share good practices identified in this exercise.

Inside the Bank, the findings from this exercise will inform the FPC's thinking around system-wide policy issues related to climate risk and the Committee's work in supporting the financial system's role in the economy's transition to net zero. The findings will also inform the PRA's supervisory policy and approach.

Outside the Bank, key lessons and themes emerging from the exercise will be shared with the UK Government and the Bank's international peers, helping to advance global thinking on how to manage climate-related financial risks, including around the appropriate role of bank and insurer capital requirements.

Scope

Given the focus of the exercise on driving improvements in risk management and understanding how firms may respond to the risks they could face, the CBES incorporated some key differences in design relative to climate stress tests run elsewhere.

The exercise required participants to make granular assessments of their largest counterparties; particular emphasis was placed on banks' and insurers' ability to evaluate the net-zero transition plans of their corporate

counterparties; and the exercise focussed on participants' responses to climate risks to a greater extent.

For banks, loss projections were focussed was on the credit risk associated with their lending activities, with an emphasis on detailed analysis of risks to large corporate counterparties. For insurers, the focus was on changes in the value of invested assets and the impact on insurance claims.

Given the difficulties inherent in accurately assessing climate risk, and the fact that this was the first detailed climate exercise involving both banks and insurers that the Bank has run, the CBES did not aim to evaluate the full impact on participants' income and capital positions.

Some factors were not included in the CBES. Examples of omissions include potential trading losses, and detailed projections of the impact of climate risks on banks' risk-weighted assets.

Loss projections for the CBES scenarios are based on the balance sheets of participants as they stood at the end of 2020. So they represent an expectation of losses that might materialise if banks and insurers do not act to reduce the climate risks they face.

This design feature makes interpretation of the results more straightforward and allows a clear, separate focus on specific actions that participants might take in response to the scenarios. But it is also likely to push projected losses upwards, as over the thirty year horizon of the CBES participants would likely be able to adjust their business models, and may reduce or mitigate some of the risks they face.

Scenarios

There are two key types of risk associated with climate change: the risks that arise as the economy moves from a carbon-intensive one to net-zero emissions, known as transition risks; and risks associated with the higher global temperatures likely to result from taking no further policy action, known as physical risks.

The CBES includes three scenarios exploring both transition and physical risks, to different degrees. These scenarios build on the climate scenarios developed by the Network for Greening the Financial System (NGFS). The CBES also includes an exercise to explore climate litigation risk facing general insurers, separate from these three scenarios.

The exercise considered two possible routes to net-zero carbon dioxide emissions globally by 2050: an Early Action scenario and a Late Action scenario. These scenarios primarily explore transition risks from climate change:

Early Action (EA): Under this scenario, climate policy is ambitious from the beginning, with a gradual intensification of carbon taxes and other policies over time.

Global carbon dioxide emissions are reduced to net-zero by around 2050 and global warming (relative to pre-industrial levels) is successfully limited to 1.8°C by the end of the scenario, falling to around 1.5°C by the end of century.

The required adjustment in the economy creates a temporary headwind to growth but this dissipates in the latter half of the scenario once a significant portion of the required transition has occurred, and the productivity benefits of green technology investments begin to be realised.

Late Action (LA): The implementation of policy to drive the transition to a net-zero economy is assumed to be delayed by a decade under this scenario.

Policy measures are then more sudden and disorderly as a result of the delay. Global warming is limited to 1.8°C by the end of the scenario (2050) relative to pre-industrial levels, but then remains around this level at the end of the century.

The more compressed nature of the reduction in emissions also results in material short-term macroeconomic and financial markets disruption. UK unemployment rises to 8.5% and the economy goes into recession for a short period. Falls in output are particularly concentrated in emissions-intensive sectors.

In both these scenarios, climate risks have been managed by 2050. In reality, however, the effectiveness of climate policy is not certain.

Based on climate simulations and modelling of the impact of policy, the early action policy path has the highest probability of success in terms of limiting climate change.

From a practical perspective, acting late would leave less time to fine-tune policy as its effectiveness was revealed, and leave governments more exposed to the risk of policy co-ordination failure.

A third scenario explores the physical risks that would begin to materialise if governments around the world fail to enact policy responses to global warming and no additional action is taken to address climate change.

In contrast to the two transition scenarios, risks in the NAA scenario continue to build beyond the end of the scenario, making it more difficult to compare the effects of such a scenario.

Furthermore the scenario does not factor in other potential geopolitical impacts of severe climate change such as increases in migration and conflict, which alongside their enormous human costs, are likely also to result in further financial losses.

No Additional Action (NAA): This scenario primarily explores physical risks from climate change. It is a deliberately severe scenario, being based on climate outcomes that would only occur later this century under the assumption that no additional action is taken to address climate change, and represents a worse than expected outcome even under such conditions.

The absence of transition policies in this scenario leads to a growing concentration of greenhouse gas emissions in the atmosphere and, as a result, global temperature levels continue to increase, reaching 3.3°C higher relative to pre-industrial levels by the end of the scenario.

This leads to chronic changes in precipitation, ecosystems and sea-levels, which are unevenly distributed globally, and in some cases irreversible. There is also a rise in the frequency and severity of extreme weather events. There are permanent impacts on living and working conditions, buildings and infrastructure. As a result, UK and global GDP growth is permanently lower and macroeconomic uncertainty increases.

Reflecting the fact that the future looks materially worse at the end of the scenario, with the adverse effects of climate change set to worsen further, UK and US equity prices are respectively just under 20 and 25% lower than they might otherwise be.

Climate Risk Management

UK banks' and insurers' approaches to projecting losses in the CBES, taken together with other qualitative information provided, suggest that participants are making good progress in some aspects of climate risk management. And there is evidence that this exercise has spurred on participating firms to develop their risk management capabilities further.

But the Bank's assessment is that UK banks and insurers still need to do much more fully to understand and manage their exposure to climate risks, including through getting data on and understanding their counterparties' and customers' transition plans.

The findings are consistent with the PRA's assessments in relation to firms' progress against a Supervisory Statement the PRA issued in 2019 (SS3/19), which sets expectations for how banks and insurers should incorporate climate risks into their risk management practices and governance arrangements, which were set out in the PRA's Climate Change Adaptation Report 2021.

In order to produce better estimates of climate risks in their portfolios, banks and insurers will need to prioritise investment in their climate risk assessment capabilities, both by focusing on their internal modelling and data capabilities and doing more to scrutinise data and projections supplied by third-party providers (upon which participants have relied heavily to compile CBES submissions).

The inability to capture appropriate and robust data in certain areas is a common limitation, which means many climate risks are only being partially measured.

Examples of gaps include information about the location of corporate assets to permit physical risk assessment, and a lack of standardised information about value chain emissions relating to corporate counterparties.

Banks and insurers will need to prioritise progress on data and will need to put in place interim measures to inform risk management until these data challenges are resolved. The Bank will continue to be supportive of co-ordinated initiatives to fill such data gaps.

A more developed and nuanced approach to risk management would allow banks and insurers to reflect climate risks more accurately in their business decisions (for example by explicitly incorporating possible future carbon prices and their impact on counterparties in pricing, lending and investment decisions).

This is important for their own long-term profitability and hence financial resilience. And it is also important to ensure that banks and insurers can support the economy in the transition to net zero.

Absent these improvements, there is a risk that banks and insurers may resort to actions that do not appropriately reflect climate risks, such as withdrawing finance to those carbon-intensive businesses in need of external finance to support their transition to less carbon-intensive production. This could give rise to wider macroeconomic risks.

The Bank will help the banks and insurers it regulates to use the results of the CBES to improve their climate risk management capabilities, both through individual firm supervisory dialogue and by sharing and discussing key thematic findings with the banking and insurance industry more broadly (including through the Climate Financial Risk Forum (CFRF)).

Exposures to climate risks

The loss estimates presented here are based on the simplifying assumption that banks' and insurers' balance sheets stay fixed over the scenario horizon, remaining as they stood at end-2020. In reality, banks and insurers business models are likely to respond to climate risks over time. These responses may act to mitigate some of the losses projected.

Across scenarios, participants' projections show that if banks and insurers do not respond effectively, climate risks could cause a persistent and material drag on their profitability.

Loss projections vary across participants and scenarios, but are equivalent to an annual drag on profits of around 10-15% on average. Losses of this magnitude could make individual firms, and the financial system overall, more vulnerable to other future shocks.

Due to the relative immaturity of firms' approaches and the complexity of modelling the impact of these risks, the uncertainty bands around projected losses are very large.

For example, participating firms' estimated loss rates on the same corporate customers can differ substantially, with the most conservative estimates for losses around ten times higher on average than the least conservative.

The impact of climate-related losses will depend on the time horizon over which they occur, which is also uncertain in reality. More clustered losses would have a bigger impact on banks and insurers.

Based on banks' and insurers' projections in this exercise, the overall costs to these firms from the transition to net zero should be bearable without substantial impacts on firms' capital positions – for example through a combination of lower retained earnings and increases in lending rates to sectors where risks increase, and also because not all of the losses on insurers' investments would ultimately fall on shareholders. Firms' projections suggest that these costs will be lower if early, well ordered action is taken.

In the case of banks, for which projections were focused on realised credit losses only, as opposed to forward-looking asset prices, loss rates were projected to rise appreciably in all three scenarios.

Banks' projected climate-related credit losses were 30% higher in the Late Action (LA) scenario than the Early Action (EA) scenario. Loss rates in the LA scenario were projected to more than double as a result of climate risks – equivalent to an extra c.£110 billion of losses for participating banks over the period. Around 40% of these losses were realised during the first five years of transition.

Key drivers were the large increase in carbon prices contained in this scenario, which leads to large corporate loan losses across energy users and energy producers, and the economy-wide recession, including a rise in unemployment and fall in house prices caused by the sharp adjustment process, leading to significant mortgage impairments. These household losses were particularly heavily concentrated in the first five years after the delayed start of the transition.

At a corporate sectoral level, the industries in which banks projected the highest loss rates in the two transition scenarios were mining (including extraction of petroleum and natural gas), manufacturing, transport and wholesale & retail trade.

On average these sectors were projected by banks to have cumulative impairment rates of 35%, more than twice the aggregate projected impairment rate on corporate portfolios.

Insurers projected heavy corporate bond and equity losses in similar sectors, with assets in the mining of gas and oil sector suffering by far the largest losses. These sectoral results were in line with expectations given the carbon intensity of these industries' supply chains.

The NAA scenario also results in significant costs for banks and insurers during the scenario horizon, as the intensification of physical risks leads to higher losses on lending and insurance activities, and lowers the return on financial assets.

In contrast to the two transition scenarios, the NAA scenario only captures a subset of the costs of climate change, which would build far into the future beyond the 30-year horizon of the exercise and persist indefinitely. And the scenario does not factor in other potential geopolitical impacts of severe climate change such as increases in migration and conflict, which alongside the enormous human cost, are likely also to result in further financial losses.

Under the NAA scenario, impairments rates projected by banks were just over 50% higher than normal levels. But these estimates are particularly uncertain. In part that is because banks appeared less well equipped to assess thoroughly the impact of physical risks prominent in the NAA scenario, particularly those arising from corporate vulnerabilities.

The aggregate results show that, for life and general insurers, the NAA scenario would be likely to have a more significant impact than either of the transition scenarios, even within the 30-year window of the exercise. For life insurers, this was because forward-looking asset price impacts are greatest at the end of that scenario with an overall impact worth just over 15% of total market value.

Such falls in asset prices would of course affect all holders of assets and participants in these markets. For general insurers, the key way that losses materialised was via a build-up in physical risks, which resulted in higher claims for perils such as flood and wind-related damage.

UK and international general insurers, respectively, projected a rise in average annualised losses of around 50% and 70% by the end of the NAA scenario. Staff analysis on UK insurance losses suggests increases could be as much four times higher than firms submitted.

Insurers reported that the impact of these increased domestic and international insurance claims would fall, ultimately, on households and businesses through higher insurance premiums or through lower availability of insurance cover.

Projected loss rates from individual banks and insurers spanned a wide range. This suggests significant uncertainty around the true magnitude of these risks, reflecting the fact that participants' climate risk assessment techniques are still developing, as well as the wide range of approaches taken by participants. The significant degree of uncertainty is corroborated by sensitivity analysis conducted by the Bank.

This exercise also highlighted data gaps and potential risks to international general insurers from climate-related litigation, which could impact the cost and availability of Directors' & Officers' liability insurance cover.

An increase in climate litigation risk would clearly also affect those businesses being litigated against beyond the insurance sector.

Challenges to business models and participants' responses to scenarios
By examining jointly the potential responses of banks and insurers to climate risk, the results of the CBES shed light on the possible collective impact of participants' behaviours, including whether they may give rise to unintended or undesirable system-wide consequences.

UK banks and insurers typically expected to respond to the scenarios in this exercise by following their existing plans around the transition to net-zero emissions, including in this instance by increasing counterparty engagement to support the transition.

In this exercise, banks and insurers planned to reduce their exposure to carbon-intensive sectors, with banks projecting the largest reductions in the petroleum and gas extraction, petroleum manufacturing, and mining and quarrying sectors. The sectors that banks and insurers planned to reduce their exposure to were broadly similar across all three scenarios.

These strategies raise the possibility that some corporate sectors (particularly some carbon-intensive ones) may struggle to access finance as the transition progresses, especially from banks. Unless the transition is carefully managed, this could have significant impacts on businesses and consumers, and through them the financial sector.

For example there could be potential macroeconomic consequences if limits in the supply of finance and insurance to fossil fuel producers could outpace the new investment in sustainable energy alternatives and improvements in energy efficiency.

Participating firms identified more business opportunities in the transition scenarios than in the NAA scenario. And banks were able to quantify more new opportunities than life insurers in this exercise.

Life insurers noted that their ability to seize some investment opportunities would be dependent upon improvements in disclosures. Some insurers expressed a concern that a surge in 'green' investment could unduly raise asset prices.

In the two transition scenarios, banks planned to increase lending substantially to some components of the gas and electricity supply sector, specifically to renewable energy firms and those developing technology for electric vehicle batteries.

At the same time, banks planned to reduce lending to firms within this sector that were particularly reliant on revenues from fossil fuels. They also envisaged increasing lending to the construction sector, reflecting greater investment in retrofitting and flood defence improvements.

Banks also planned to expand into retail lending opportunities created by the transition, including offering green mortgages, and providing financing products for home energy efficiency improvements.

General insurers also planned to expand further into opportunities that would be created by a net-zero transition, for example by providing insurance to renewable energy projects, and to companies developing battery and fuel cell technology.

In the NAA scenario, banks and insurers generally sought to reduce their exposures to similar sectors as in the transition scenarios. General insurers planned to increase the price of insurance to reflect the increases in physical risk in the scenario.

These firms' insurance contracts are typically written to cover one year, allowing them to alter pricing relatively quickly as risks change. And insurers noted that UK household flood insurance coverage could fall

sharply in such a scenario, particularly as insurance on some properties would become unaffordable once the Flood Re scheme ended as per current legislation in 2039, though the vast majority of households would still be able to afford insurance.

In the NAA scenario participants' responses indicated that around 7% of UK households that they currently cover could be forced to go without insurance – because their properties become uninsurable, or because they cannot afford insurance at the prices offered. The share of households affected could be greater than this, to the extent that general insurers have underestimated the physical risk impact of the NAA scenario.

Households and corporates that insurers become unwilling to insure, or where insurance premiums become unaffordable, may face difficulty in accessing finance from banks. UK households in regions most exposed to physical risk would face challenges re-mortgaging their properties in the NAA scenario because they would fall in value due to severe flooding and/or become uninsurable.

45% of the mortgage impairments in the scenario are accounted for by just 10% of the 4-digit postcode areas analysed. Affected households may find themselves stranded on the more expensive Standard Variable Rate mortgages.

Both banks and insurers noted that these risks could be in part mitigated by investment in flood defences, increasing flood resilience measures for properties, and encouraging flood-resilient repairs. They also noted their support for a continuation of a publicly supported UK flood reinsurance pool in such a scenario, and an extension to include properties built after 2009.

The Bank will work with the Government and the FCA to support greater understanding of risks to the provision of financial services highlighted by the CBES exercise.

To read more: https://www.bankofengland.co.uk/stress-testing/2022/results-of-the-2021-climate-biennial-exploratory-scenario

'Sharing my screen cost me £48,000' – half of investors would miss signs of screen sharing scam as FCA warns of 86% increase

With over £25 million lost so far, the FCA launches its latest ScamSmart campaign aimed at raising awareness of increasingly sophisticated investment scam tactics:

- A 59-year-old woman lost £48,000 as scammers used screen sharing software to take over her computer and access her banking history.
- Her case is one of 2,142 the FCA has seen since July 2020, with over £25 million lost between 1 January 2021 and 31 March 2022 and victims ranging from 18 to over 70.
- The FCA's latest ScamSmart campaign aims to raise awareness of these tactics and help investors spot the warning signs by checking its Warning List.
- Its research shows 51% of investors would check the FCA's Warning List before making an investment – but 47% would not see a request to use software or an app to access their device as a red flag.

What are screen sharing scams?

A screen sharing scam is the method a scammer might use to take information from you or access your accounts to transfer your money. You may be contacted out of the blue through social media or over the phone. Or when searching online for an investment opportunity or the contact details for a company.

Once a scammer has contacted you, they will try and gain your trust and convince you they can help. The type of scams may vary, whether that's help with an investment or a banking service, the scammer will typically ask you to download legitimate screen sharing software.

This could be software you have heard of or have used before with work, friends or family. Examples of this type of software include, but are not limited to, AnyDesk, Microsoft Teams, TeamViewer, Zoom. This could be through your phone, laptop or computer.

The scam can only take place if you download the software and allow them to take control of your screen. Once they have access to your screen, they can access to your personal information. Including any financial accounts, such as your online banking.

New research from the FCA has found that nearly half (47%) of investors would fail to identify a screen sharing scam, as it reveals an increase of 86% in cases in one year, with 2,014 cases and over £25 million in loses.

In one case, a 59-year-old who was persuaded to download remote desktop software to secure an investment, lost over £48,000 while scammers accessed her banking details, her pension, and applied for loans on her behalf.

Angela Underhill clicked on an advertisement for bitcoin and received a call from individuals claiming to be financial advisers. Offering to complete the first investment for her, they asked her to download the 'AnyDesk' platform, which then gave the scammers open access to all the financial details on her computer.

Her case is just one of thousands the FCA has seen reported to its Consumer Helpline. Using platforms including Teams, TeamViewer and Zoom, screen sharing scams not only involve consumers sharing their financial data – but scammers have also been able to embed themselves in victims' digital devices to access online banking and investment details.

To understand what might be influencing potential victims, the FCA surveyed 2,000 investors from the ages of 18 to 55+.

The results showed that 51% of would-be investors would check if a company appears on the FCA's Warning List when deciding if an investment opportunity is legitimate.

The FCA's Warning List is a list of firms that are not authorised or registered by the FCA, and are known to be running scams.

However, of the 91% who said they would never share their PIN with a stranger, 85% would not think a request by a website to use or download software as a warning sign that someone was seeking to gain illegal access to personal information on your device.

Likewise, while 88% said they would check if their investments were offered or sold by FCA firms , 10% of these people would still trust their gut instinct with an investment opportunity from someone they didn't know without making proper checks, like ensuring the firm or the financial promotion is properly authorised.

With the pandemic increasing use of video conferencing and remote platforms to both work and socialise, scammers are taking advantage of a growing familiarity with requests for screen sharing.

Although older respondents admitted needing more help with technology, younger investors are not immune: a quarter (26%) of those aged 18-34 would agree to screensharing their online banking or investment portal with someone they had not met.

Mark Steward, Executive Director of Enforcement and Market Oversight, FCA, said: 'Investment scams can happen over many months, but sharing your screen without making the proper checks can change everything in an instant. Once scammers gain to your screen, they have complete control.

That means access to your sensitive banking and investment information, the freedom to browse at their leisure, and the ability to take whatever details they want.

It can affect any investor, no matter how experienced. It's incredibly difficult to get money back once lost in this way, but there are ways to protect yourself: don't share your screen with anyone, as legitimate firms will not ask you to do this and check out our Scamsmart website for advice on how to avoid being scammed.'

The research also revealed other factors which might tempt investors to make a snap decision: 23% said they would be encouraged if the person they were speaking to appeared knowledgeable about investing; 17% said the possibility of securing better returns than elsewhere, and 14% would be encouraged if that person appeared to be successful – with displays of wealth.

The FCA is calling on all investors to be ScamSmart and check the advice on our Scamsmart website, including our Warning List before making any investment decisions.

This will help identify any firms that are actively running scams, or flag to investors where additional research is needed.

If you deal with an unauthorised firm, you will not be covered by the Financial Ombudsman Service or Financial Services Compensation Scheme (FSCS) if things go wrong.

There are three important questions to ask to protect yourself from these scams:

1. Have you checked the FCA's Scamsmart wesbite and Warning List? This will help you to avoid being scammed and show you whether or not the firm you are dealing with is registered, or known to be suspicious.

2. Are you being asked to download anything new? Your bank will never need to access your screen to view your information, so someone asking you to do this is a clear warning sign.

3. Have you navigated away from your banking, or investment platform? Anything that takes you away from your banking or investment app, and through a search engine, increases the risk of coming across a fraudulent number or link.

To read more: https://www.fca.org.uk/news/press-releases/investors-miss-screen-sharing-scam-signs

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

United States Senate Committee on
Homeland Security & Governmental Affairs
U.S. Senator Gary Peters | Chairman

Ransomware is a dangerous form of cyber-attack where threat actors prevent access to computer systems or threaten to release data unless a ransom is paid.

It has the power to bankrupt businesses and cripple critical infrastructure – posing a grave threat to our national and economic security.

The use of cryptocurrencies has further enabled ransomware attacks, particularly because cryptocurrency is decentralized and distributed and illicit actors can take steps to obscure transactions and make them more difficult to track.

In recent years, ransomware attack victims have included hospitals, school systems, local, state, and federal government agencies, as well as other critical infrastructure, including the water and energy sectors.

In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States.

According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."

Many of these attacks generated significant losses and damages for victims. A threeyear comparison of the number of complaints of ransomware submitted to the Federal Bureau of Investigation (FBI) between 2018 and 2020, demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses.

In 2021, the agency received 3,729 ransomware complaints with adjusted losses of more than $49.2 million. However, even these figures likely drastically underestimate the actual number of attacks and ransom payments made by victims and related losses.

In fact, the FBI acknowledges that its data is "artificially low." Further evidence of this under-reporting is that the government data is significantly lower than several private sector estimates.
For instance, Chainalysis, a blockchain data and analysis company that works with financial institutions, insurance and cybersecurity companies, and as a contractor for the U.S. government, reports that in 2020, malign

actors received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, close to a 300 percent increase over a two-year period.

A separate study by the anti-malware company Emsisoft found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.

To better understand this growing threat, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced in July 2020 an investigation into the role of cryptocurrency in incentivizing and enabling ransomware attacks, and the resulting harm of such attacks to victims.

As a part of this ten-month investigation, Committee staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands.

While not exhaustive, this report addresses key pieces of the larger landscape of the increasing national security threat from ransomware attacks and the use of cryptocurrency for ransom payments.

The report details recommendations to address current gaps in information on ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

The report finds that there is a lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

While multiple federal agencies are taking steps to address the increasing threat of ransomware attacks, more data is needed to better understand and combat these attacks.

In interviews with Committee staff, federal officials and private sector companies each acknowledged the need for more compliance and data (e.g., reporting of incidents and ransom payments).

When more data is collected, the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery.
Such information also facilitates more efficient investigation and prosecution of illicit actors.

To address the current lack of information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member

Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022.

The incident reporting provisions later became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the Consolidated Appropriations Act of 2022 in March 2022. The new reporting mandates in the law will begin to address this problem.

Nevertheless, as indicated by the findings in the report, the Administration and Congress must remain vigilant against this growing threat. Almost 40 million Americans – including approximately three-in-ten Americans age 18 to 29 – have engaged in some form of investment, trade, or other legitimate use of cryptocurrencies according to a November 2021 estimate by the nonpartisan Pew Research Center.

The global market value of all cryptocurrencies reached $3 trillion in 2021, up from $14 billion in 2016. However, according to multiple agencies interviewed by Committee staff, cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of money from victims across diverse sectors with incredible speed.

The payment structure's decentralized nature, as well as irregular regulatory compliance by some entities within the space and new anonymizing techniques contribute to the challenges law enforcement faces when seeking to arrest criminal actors, particularly foreign-based actors.

High profile attacks, such as Colonial Pipeline, demonstrate ransomware attackers' threat to national security. The FBI's recovery of over half of the ransom paid by Colonial Pipeline, however, shows that with access to the right information, law enforcement can leverage cryptocurrency's unique features as well as other investigative techniques to track down cyber criminals and recover stolen funds.

Unfortunately, data reporting and collection on ransomware attacks and payments is fragmented and incomplete. Two federal agencies claim to host the government's one stop location for reporting ransomware attacks – the Cybersecurity and Infrastructure Agency (CISA) StopRansomware.gov website and the FBI's IC3.gov.

These two websites are separate and, while the agencies state that they share data with each other, in discussions with Committee staff, ransomware incident response firms questioned the effectiveness of such communication channels' impact on assisting victims of an attack.

Many federal regulators have taken steps to address the rising threat of ransomware attacks by issuing new, and expanding existing, regulations and guidance.

Generally, with respect to cryptocurrency, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has clarified that "money service businesses", e.g., persons that accept and transmit "value that substitutes for currency", are subject to key financial regulations.

Over the past few years, the Securities and Exchange Commission (SEC), Internal Revenue Service (IRS), and FinCEN have each issued new guidance and regulations subjecting cryptocurrency to additional oversight.

In 2021, the Department of Justice (DOJ), SEC, and the Treasury Department's Office of Foreign Assets Control (OFAC), among other agencies, also issued guidance recognizing the need for more ransomware incident reporting.

On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies. Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity."

The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, however, is fragmented and incomplete.

This limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security and limits private sector and federal government efforts to assist cybercrime victims.

As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows. Approximately 74 percent of global ransomware revenue in 2021 went to entities either likely located in Russia or controlled by the Russian government.

Further, CISA and other federal agencies have warned that Russia's invasion of Ukraine could lead to additional malicious cyber activity, including ransomware attacks, in the United States.

Therefore, as the report finds, prioritizing the collection of data on ransomware attacks and cryptocurrency payments is critical to addressing increased national security threats.

FINDINGS OF FACT

1. The federal government lacks comprehensive data on ransomware attacks and use of cryptocurrency in ransom payments.

The government largely relies on voluntary reporting of ransomware attacks and cyber extortion demands, which only captures a fraction of the attacks that occur.

As of July 2021, the Cybersecurity and Infrastructure Security Agency (CISA), which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.

2. Current reporting is fragmented across multiple federal agencies.

Data on ransomware attacks is reported to numerous federal agencies including CISA, the FBI, and the Treasury Department's FinCEN, among others. These agencies do not capture, categorize, or publicly share information uniformly.

3. Lack of reliable and comprehensive data on ransomware attacks and cryptocurrency payments limits available tools to guard against national security threats.

The lack of data on ransomware attacks and cryptocurrency ransom payments blunts the effectiveness of available tools for fighting ransomware attacks including U.S. sanctions, law enforcement efforts, and international partnerships, among other tools.

4. Currently available data on ransomware attacks and cryptocurrency payments limits both private sector and federal government efforts to assist cybercrime victims.

The private sector and the federal government are not able to fully and effectively assist victims to prevent or recover from ransomware attacks without a comprehensive dataset on ransomware attacks, ransom demands, and payments. Such a dataset does not currently exist.

RECOMMENDATIONS

1. The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.

CISA should complete the required rulemaking as soon as possible to implement the requirements in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law as part of the Consolidated Appropriations Act of 2022, which mandates incident reporting of substantial cyber-attacks and ransomware payments against critical infrastructure.

Federal agencies should implement the requirement in the law to share all cyber incident reports with CISA to enable a consolidated view of incidents from across different sectors and reported under different regulatory regimes.

2. The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.

Agencies should standardize how data from existing reporting requirements for ransomware incidents and ransom payments is organized and formatted across federal government agencies to enable more comprehensive information sharing and analysis.

3. Congress should establish additional public-private initiatives to investigate the ransomware economy.

The federal government should promote public-private partnerships to research the ransomware economy, in particular, the interrelationships between cybercriminals who conduct or facilitate ransomware attacks and the financial structures facilitated by cryptocurrencies that sustain cybercriminals' illicit activities, including privacy coins.

These partnerships should also examine ransomware infrastructure to help design and promote effective countermeasures.

4. Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.

Congress and relevant agencies should consider ways to support partners within the private, nonprofit, and academic sectors seeking to expand the collection and organization of information on ransomware attacks including by examining federal funding options and sharing anonymized data regarding ransomware attacks and payments.

In addition, government agencies should collaborate with partners to identify viable crowdsourcing initiatives to pool information regarding ransomware attacks and extortion payments.

You may visit:
https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf

Green Swan 2022, watch the videos!

A virtual conference co-organised by the Bank for International Settlements, the European Central Bank, the Network for Greening the Financial System and the People's Bank of China

Building on the foundation of the inaugural Green Swan Conference in 2021, which brought together a wide range of high-calibre policymakers, experts and practitioners from different sectors, Green Swan 2022 offers a deeper dive into the topics of:

- (i) monetary policy setting and operations in the context of climate change, and
- (ii) the role of finance in the climate transition, including transparency and disclosures, transition plans and financing green innovation.

After an introduction to the Green Swan Conference by Luiz Pereira, Ravi Menon explains why it is imperative for central banks and supervisors to consider climate-related risks in fulfilling their mandates. In his capacity as Chair of the Network for Greening the Financial System, he also highlights the 2022-24 work programme for the NGFS.

You may visit: https://www.youtube.com/watch?v=fHmcp-cx-9M&t=3s

Session 1: The role of finance in climate transition

The role and potential of the financial sector in climate change and the carbon market.

In his keynote speech, Zhou Xiaochuan highlights how a massive mobilisation of financial resources, as well as the appropriate incentives, are needed for the transition. Carbon pricing and trading have an important role to play on a global scale.

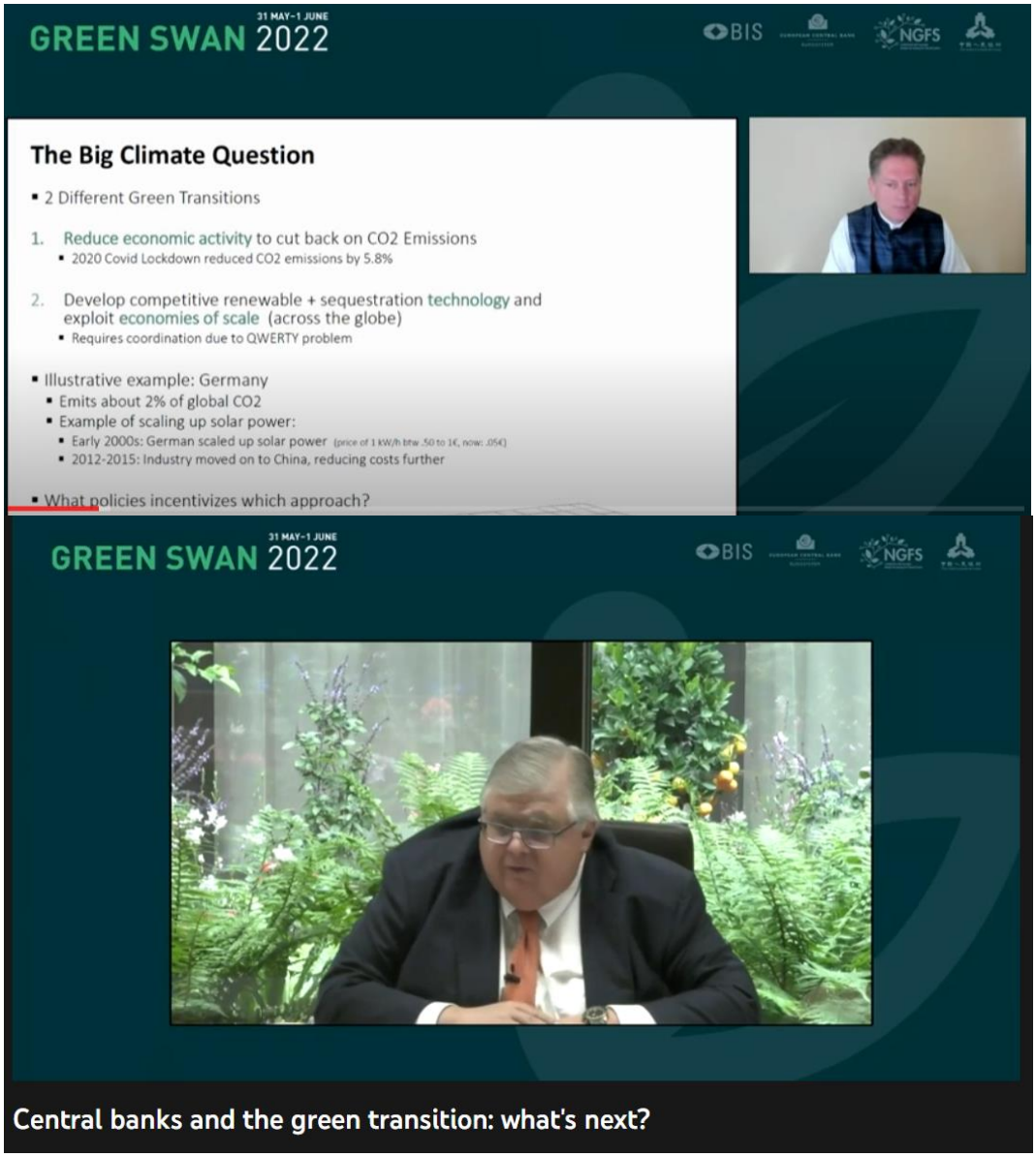
You may visit: https://www.youtube.com/watch?v=CeY9EpAU5q8&t=7s

What can the public and private sectors do to turn transition finance frameworks to actions?

In this roundtable discussion, experts from different fields analyse issues relating to financing the green transition, spanning from market failures to the need for climate justice, from regional considerations to the need for international cooperation.

You may visit: https://www.youtube.com/watch?v=U3u3ItARu2w

To find all the presentations you may visit:
https://www.bis.org/events/green_swan_2022/overview.htm



Staff Working Paper No. 984

An interpretable machine learning workflow with an application to economic forecasting

Marcus Buckmann and Andreas Joseph

BANK OF ENGLAND

Predictive machine learning models are increasingly being used at decision-making institutions, such as central banks, governments and international institutions (Doerr et al., 2021).

Major appeals of these models are that they often give more accurate predictions than conventional approaches and can handle high-dimensional data (Haldane, 2018).

On the downside, many machine learning methods suffer from the black box critique. It is not straightforward to assess the factors driving predictions and therefore to understand the relations between the inputs and output of the model. However, this understanding of a model is crucial, especially for decision making processes, for several reasons.

First, both decision makers and their audiences naturally have a desire to understand the inputs leading to decisions and legitimise them.

Second, decision making processes often involve multiple models. The information derived from different models should be compatible leading to a coherent picture. The understanding of all models involved is needed for this.

Third, models can ‘misfire’ for several reasons, for example by picking up spurious relations in the data.

This often can only be detected and prevented if one has a good understanding of a model.

Prediction models whose accuracy is a key motivation behind their deployment— which often holds for machine learning methods—should also help to inform the narrative approach behind any economic policy decision rather than providing mere black box predictions (George, 1999; Burgess et al., 2013; Independent Evaluation Office, 2015).

Machine learning models also can provide a richer set of information compared to more conventional statistical models, like linear regression models.

In particular, they can implicitly learn nonlinear functional forms and interaction from the data without the need to specify them a priori.

In this paper, we lay out a multi-step workflow for the use of machine learning models, which we deem suitable to inform decision making processes. It consists of three steps which can be directly applied to other contexts as well than those presented in the accompanying case study.

First, a model comparison is conducted between conventional statistical methods and machine learning models to provide prima facie evidence of whether a machine learning approach is likely to deliver benefits. If the primary objective is model accuracy, e.g. for forecasting, this would be a model horse race to minimise the forecasting error.

Second, the machine learning predictions are decomposed into the contributions of the individual model variables. This allows us to uncover the relative importance of variables and understand the functional forms learned by the different machine learning models. By a comparison across models, one can gauge how robust feature decompositions are to the choice of the algorithm.

Third, statistical inference is conducted to understand which variables make a statistically significant contribution to the accuracy of a model, providing a level of confidence for our interpretations and any narrative attached to them. This inference uses a parametric regression analysis, allowing for a standardised communication of statistical model results.

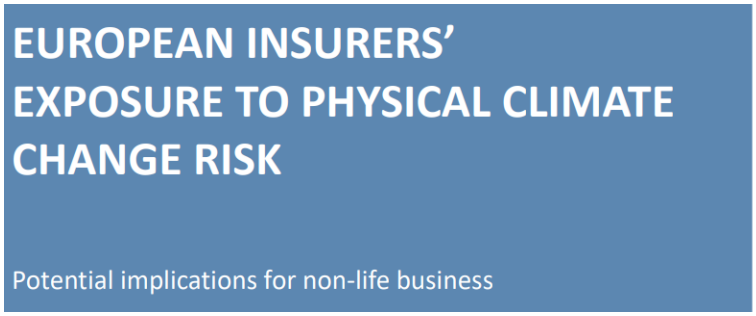
The paper: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2022/an-interpretable-machine-learning-workflow-with-an-application-to-economic-forecasting.pdf?la=en&hash=829CF4A26BD34A1176432F07385890EB02A5EEB8

EIOPA assesses European insurers' exposure to physical climate change risks

The report presents the first results based on a large data collection exercise from the industry. It focuses on property, content and business interruption insurance against windstorm, wildfire, river flood and coastal flood risks.

These risks have been identified as the most relevant and potentially most disruptive for the European property insurance business under a current and forward-looking perspective.

The report aims to provide an initial assessment of the European insurance sector's exposure to climate-related hazards and inform future work in this relatively new field.



The results indicate that European groups and solo undertakings included in the sample have been historically well placed to handle claims stemming from three major European natural catastrophes analysed in the report.

However, it is important to note that the insurance sector's ability to continue to offer financial protection against the consequences of such events relies on their ability to measure the likely impact of climate change and adapt their business strategies.

Participants surveyed for the paper said they expect all property-related lines of business to be impacted by physical climate change risks. There is an emerging consensus among them that premiums are likely to increase and that adaptation and mitigation measures will play a crucial role in reducing risk levels in the future.

Finally, the report's findings show that there is still work to do for the insurance industry to prepare for climate-related changes. EIOPA will continue its work with national competent authorities and the industry to raise awareness and contribute to the sector's preparation for the effects of climate change.

CLIMATE CHANGE AND PHYSICAL RISKS: THE "NEW NORMAL" IN THE INSURANCE SECTOR

Table 1: Examples of chronic and acute climate-related hazards

	Temperature-related	Wind-related	Water-related
Chronic	• Changing temperature (air, freshwater, marine water) • Heat stress • Temperature variability • Permafrost thawing	• Changing wind patterns	• Changing precipitation patterns (rain, hail, snow/ice) • Precipitation and/or hydrological variability • Sea level rise • Water stress
Acute	• Heatwaves • Cold waves/frost • Wildfire	• Tropical cyclone • Windstorm (including blizzards, dust and sandstorms) • Tornado	• Drought • Heavy precipitation (rain, hail, snow/ice) • Flood (coastal, fluvial, pluvial, ground water)

Source: Extract from Final report of the EU Technical Expert Group on Sustainable Finance (TEG, 2020)

The impacts of global warming on natural and human systems are already visible today. Warming from anthropogenic emissions are likely to cause further long-term changes such as rising temperatures, sea levels, and increase in frequency, severity and correlation of natural catastrophes and climate-related extremes (e.g. heat waves, heavy precipitation, droughts and storm surges) in many European regions, and worldwide.

The effects of these climate-related changes on the pricing and underwriting of risks are likely to be substantial for a sector whose business model involves offering financial protection against the consequences of such events.

Physical climate change risks are the risks that arise from the physical effects of climate change.

These can affect both the asset and the liability side of insurers' balance sheet. On the asset side, the increase in frequency and severity of extreme weather events across different perils may impact insurers for instance through direct property investments.

On the liability side, physical risk is likely to have pricing, revenue and claim implications. Higher than foreseen claims would also increase the insurers' underwriting and liquidity risks and put pressure on capital levels.

The impacts of climate change on physical risk could arise from both an increase of extreme weather events (acute impacts), as well as from gradual global warming (chronic impacts).

Table 1 summarises the key impacts. Acute impacts can lead to damage to property, business disruption or reduced productivity. Chronic impacts, particularly from increased temperatures, sea levels rise and precipitation, may affect labor, capital and agriculture productivity.

While progress is being made in terms of understanding the potential consequences of both acute and chronic impacts on the insurance sector, many challenges remain.

First, the expected increase in global temperature needs to be translated into changes in frequency and severity of weather-related catastrophes as well as in chronic effects such as sea-level rises.

Second, these estimations need to be converted into economic impacts on the undertaking's underwriting portfolio in relevant geographical areas.

Third, a view and understanding on the relevant time horizons over which climate-related risk are most likely to materialise are essential.

Finally, the insurance business is also likely to evolve in the long-term to better adapt to climate change risks and opportunities.

For these reasons, an accurate assessment of physical climate-change related risks requires access to a unique set of granular data, scientific and actuarial expertise, new modelling methods as well as a deep understanding of the various business models employed in the insurance sector.

While an overall assessment is outside the scope of this discussion paper, the next section explains three key components required for an initial assessment of physical risks in general terms.

Physical risk analysis in light of climate change

When modelling physical climate-change risks, three key factors need to be considered: the level of exposure estimating the potential share and composition of the population or the value and properties of assets at risk, the hazard describing the physical characteristics, such as frequency and intensity, of weather-related events and the vulnerability of the exposures to weather-related damages.

To estimate the level of risk, information on the changes in hazard are combined with the level of exposure and its corresponding vulnerability.

Further, an increase in frequency and intensity of weather-related catastrophes alone do not necessary imply an increase in physical risk.

If, for example, there is no property or people living in the affected areas or if there are sufficient preventive measures installed, the damages caused by the event may be limited or negligible.

To read more: https://www.eiopa.europa.eu/media/news/eiopa-assesses-european-insurers%E2%80%99-exposure-physical-climate-change-risks

https://www.eiopa.europa.eu/document-library/discussion-paper/discussion-paper-physical-climate-change-risks_en

Testimony at Hearing before the Subcommittee on Financial Services and General Government U.S. House Appropriations Committee

SEC Chair Gary Gensler

Good morning, Chairman Quigley, Ranking Member Womack, and members of the Subcommittee. I'm honored to appear before you for the second time as Chair of the Securities and Exchange Commission. It is good to be here alongside Federal Trade Commission Chair Khan. As is customary, I'd like to note that my views are my own, and I am not speaking on behalf of my fellow Commissioners or the SEC staff.

The Gold Standard of Capital Markets

I'd like to open by discussing two key years in economic policymaking: 1933 and 1934.

We were in the midst of the Great Depression. President Franklin Delano Roosevelt and Congress addressed this crisis through a number of landmark policies.

Amongst them, in 1933 and 1934, Congress and FDR came together to craft the first two federal securities laws. These statutes created requirements and regulations around disclosure, registration, exchanges, and broker-dealers, and established the SEC to oversee the markets.

Additionally, in 1933, President Roosevelt formally suspended the use of the gold standard. Then, in 1934, the Gold Reserve Act was enacted, prohibiting government and financial institutions from redeeming dollars for gold.

Though it takes constant vigilance to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation, the U.S. laws became the gold standard for capital markets around the world.

In other words, in those two key years, one could say we replaced one gold standard with another gold standard: the securities laws.

The core principles of the securities markets laid out in these statutes were important for issuers and investors in our domestic markets. I believe they also contributed to America's geopolitical standing around the globe.

We are blessed with the largest and most innovative capital markets in the world. The U.S. capital markets represent 38 percent of the globe's capital markets. This exceeds even our impact on the world's gross domestic product, where we hold a 24 percent share.

What's more, U.S. market participants rely on capital markets more than market participants in any other country. For example, debt capital markets account for 80 percent of financing for non-financial corporations in the U.S. In the rest of the world, by contrast, nearly 80 percent of lending to such firms comes from banks.

We are the destination of choice for companies seeking to raise money in both public and private markets. Private capital markets, such as venture capital, have brought new ideas to market quickly and flexibly.

We can't take our leadership in capital markets for granted, though.

New financial technologies and business models continue to change the face of finance for investors and issuers. More retail investors than ever are accessing our markets. Other countries are developing deep, competitive capital markets as well, seeking to surpass ours.

Further, market participant incentives, economic cycles, and the nature of finance itself will constantly challenge even a gold standard. In recent years, we've seen as much — whether the market events of March 2020, the meme stock-related volatility in early 2021, the speculative crypto markets, the boom of special purpose acquisition companies (SPACs), or the collapse of Archegos Capital Management, which we recently charged with fraud and market manipulation.

What's more, we are in the midst of uncertain geopolitical events. On top of that, around the globe, central banks have started to transition from an accommodating to a tightening policy stance.

Given these trends, I think we should do everything we can to maintain and enhance that gold standard of the markets.

Maintaining the Gold Standard

There are two broad ways to do that, in my view.

One is to work with the Commission and staff to update our rules for modern markets and technologies as we execute our mission: to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. We must remain vigilant to opportunities to enhance competition, transparency, fairness, and resiliency.

The other way — and the main focus of today's testimony — is to ensure that the SEC is adequately resourced so we can remain the cop on the beat. The SEC is deficit-neutral, fully funding ourselves with fees on securities transactions.

Having worked in finance for decades, I'd long respected the SEC and its tremendous staff. What I couldn't fully appreciate is the sheer magnitude of this agency's work on a daily basis.

We oversee 24 national securities exchanges, 99 alternative trading systems, nine credit rating agencies, seven active registered clearing agencies, five self-regulatory organizations and other external entities.

We look after the accounting and auditing functions of the public markets, process thousands of periodic filings and registration statements, and work through thousands of examinations and enforcement actions each year. We review the disclosures and financial statements of more than 8,200 reporting companies.

Markets don't stand still. The world isn't standing still. Our resources can't stand still, either.

And yet, as I will detail, our agency has shrunk. When I testified you last year, the agency had 4 percent fewer staff than it did in 2016; it remains modestly below where it was in 2016. We can't shrink when we're trying to maintain a gold standard. The best athletes in the world still practice — generally, even more than their competitors.

Our capital markets are a national treasure. We, at the SEC, must work to maintain them as the envy of the world. But we can't do it alone. We need the help of Congress.

Growth in the Markets

The last five years have been a remarkable time in our $100-trillion capital markets. Thus, while there are many measures of market activity, by most objective measures, we should have grown during the past five years.

Instead, the opposite has happened. As our capital markets have grown, this agency has shrunk.

As just a few examples:

In the past five years, the number of registered entities we oversee has grown by 12 percent (from 26,000 to 29,000), even though the SEC has shrunk in that time.

Since 2016, the number of private funds managed by registered investment advisers has increased 40 percent, to 50,000.

The amount of data that the SEC processes has swelled by 20 percent annually for each of the last two years.

Moreover, the highly volatile and speculative crypto marketplace has mushroomed, attracting tens of millions of American investors and traders.

In 2016, there were an estimated 644 crypto tokens on the worldwide market. Five years later, that number had gone up more than tenfold.

The volatility in the crypto markets in recent weeks highlights the risks to the investing public.

Technology is rapidly changing as well. Predictive data analytics, including machine learning, are increasingly being adopted in finance — from trading, to asset management, to risk management.

Growing cybersecurity risks have implications for the financial sector, investors, issuers, and the economy at large.

Beyond that, our responsibilities have grown. Important legislation, such as the Holding Foreign Companies Accountable Act of 2020 (HFCAA), has placed additional demands on our resources. Rules implementing certain mandates of the Dodd-Frank Act of 2010 recently went into effect. Such mandates, designed to protect investors, often have been unfunded.

SEC FTE (FY 2016 - FY 2023)

	FY 2016 Actual	FY 2021 Actual	FY23 Request
SEC Overall	**4,554**	**4,459**	**4,808**
Corporation Finance	477	388	438
Economic and Risk Analysis	151	140	174
Enforcement	1,380	1,315	1,365
Examinations	1,023	1,061	1,100
Investment Management	183	200	222
Trading and Markets	258	256	290

Figure 1: Headcount (FTEs) at the SEC and in individual Divisions. Overall SEC headcount includes all Offices and Divisions.

Thus, I am pleased to support the President's Fiscal Year 2023 (FY23) budget request for SEC operations, totaling $2.149 billion, an 8 percent increase over FY22. This request would allow us to maintain current services, add full-time equivalents in critical growth areas, and devote more resources to technology. This number would support a modest

growth of (about 6 percent) in full-time equivalents (FTEs) above our previous peak in FY16, assuming consistent vacancy rates.

This increase would be modest, given the major trends affecting our markets since 2016. Moreover, to fund our operations, the agency collects fees on securities transactions at a rate intended to fully offset our appropriation.

Thanks to the work of the remarkable staff, the SEC has faced the challenges of limited resources well.

For the SEC to continue to succeed in carrying out our mission, our personnel level must continue to grow commensurate with the expansion and complexity in the capital markets around the globe.

To read more: https://www.sec.gov/news/testimony/gensler-testimony-fsgg-subcommittee

Weak Security Controls and Practices Routinely Exploited for Initial Access

Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system.

This joint Cybersecurity Advisory identifies commonly exploited controls and practices and includes best practices to mitigate the issues. This advisory was coauthored by the cybersecurity authorities of the United States, Canada, New Zealand, the Netherlands, and the United Kingdom.

Malicious cyber actors often exploit the following common weak security controls, poor configurations, and poor security practices to employ the initial access techniques.

• Multifactor authentication (MFA) is not enforced. MFA, particularly for remote desktop access, can help prevent account takeovers. With Remote Desktop Protocol (RDP) as one of the most common infection vector for ransomware, MFA is a critical tool in mitigating malicious cyber activity. Do not exclude any user, particularly adminstrators, from an MFA requirement.

• Incorrectly applied privileges or permissions and errors within access control lists. These mistakes can prevent the enforcement of access control rules and could allow unauthorized users or system processes to be granted access to objects.

• Software is not up to date. Unpatched software may allow an attacker to exploit publicly known vulnerabilities to gain access to sensitive information, launch a denial-of-service attack, or take control of a system. This is one of the most commonly found poor security practices.

• Use of vendor-supplied default configurations or default login usernames and passwords. Many software and hardware products come "out of the box" with overly permissive factory default configurations intended to make the products user-friendly and reduce the troubleshooting time for customer service. However, leaving these factory default configurations enabled after installation may provide avenues for an attacker to exploit.

Network devices are also often preconfigured with default administrator usernames and passwords to simplify setup. These default credentials are not secure—they may be physically labeled on the device or even readily available on the internet.

Leaving these credentials unchanged creates opportunities for malicious activity, including gaining unauthorized access to information and installing malicious software.

Network defenders should also be aware that the same considerations apply for extra software options, which may come with preconfigured default settings.

• Remote services, such as a virtual private network (VPN), lack sufficient controls to prevent unauthorized access. During recent years, malicious threat actors have been observed targeting remote services.

Network defenders can reduce the risk of remote service compromise by adding access control mechanisms, such as enforcing MFA, implementing a boundary firewall in front of a VPN, and leveraging intrusion detection system/intrusion prevention system sensors to detect anomalous network activity.

• Strong password policies are not implemented. Malicious cyber actors can use a myriad of methods to exploit weak, leaked, or compromised passwords and gain unauthorized access to a victim system. Malicious cyber actors have used this technique in various nefarious acts and prominently in attacks targeting RDP.

• Cloud services are unprotected. Misconfigured cloud services are common targets for cyber actors. Poor configurations can allow for sensitive data theft and even crypto jacking.

• Open ports and misconfigured services are exposed to the internet. This is one of the most common vulnerability findings. Cyber actors use scanning tools to detect open ports and often use them as an initial attack vector. Successful compromise of a service on a host could enable malicious cyber actors to gain initial access and use other tactics and procedures to compromise exposed and vulnerable entities. RDP, Server Message Block (SMB), Telnet, and NetBIOS are high-risk services.

• Failure to detect or block phishing attempts. Cyber actors send emails with malicious macros—primarily in Microsoft Word documents or Excel files—to infect computer systems. Initial infection can occur in a variety of ways, such as when a user opens or clicks a malicious download link, PDF, or macro-enabled Microsoft Word document included in phishing emails.

• Poor endpoint detection and response. Cyber actors use obfuscated malicious scripts and PowerShell attacks to bypass endpoint security controls and launch attacks on target devices. These techniques can be difficult to detect and protect against.

MITIGATIONS

Applying the following practices can help organizations strengthen their network defenses against common exploited weak security controls and practices.

Control Access

• Adopt a zero-trust security model that eliminates implicit trust in any one element, node, or service, and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. Zerotrust architecture enables granular privilege access management and can allow users to be assigned only the rights required to perform their assigned tasks.

• Limit the ability of a local administrator account to log in from a remote session (e.g., deny access to this computer from the network) and prevent access via an RDP session. Additionally, use dedicated administrative workstations for privileged user sessions to help limit exposure to all the threats associated with device or user compromise.

• Control who has access to your data and services. Give personnel access only to the data, rights, and systems they need to perform their job. This role-based access control, also known as the principle of least priviledge, should apply to both accounts and physical access.

If a malicious cyber actor gains access, access control can limit the actions malicious actors can take and can reduce the impact of misconfigurations and user errors.

Network defenders should also use this role-based access control to limit the access of service, machine, and functional accounts, as well as the use of management privileges, to what is necessary. Consider the following when implementing access control models:

o Ensure that access to data and services is specifically tailored to each user, with each employee having their own user account.

o Give employees access only to the resources needed to perform their tasks.

o Change default passwords of equipment and systems upon installation or

commissioning.

o Ensure there are processes in place for the entry, exit, and internal movement of employees. Delete unused accounts, and immediately remove access to data and systems from accounts of exiting employees who no longer require access. Deactivate service accounts, and activate them only when maintenance is performed.

• Harden conditional access policies. Review and optimize VPN and access control rules to manage how users connect to the network and cloud services.

• Verify that all machines, including cloud-based virtual machine instances do not have open RDP ports. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.

To read more:
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-137A-Weak_Security_Controls_and_Practices_Routinely_Exploited_for_Initial_Access.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.

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements.