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, July 2021

Dear members and friends,

Today we will start with EIOPA's *Insurance stress test 2021*.

EIOPA carries out regular insurance stress tests to assess how well the European insurance industry is able to cope with severe but plausible adverse development of the financial and economic conditions.

Stress test results help supervisors identify the vulnerabilities of the insurance industry and how to improve its resilience.

The 2021 stress test exercise focuses on a prolonged COVID-19 scenario in a "lower for longer" interest rate environment and evaluates its impacts on the capital and liquidity position of the entities in scope.

Objective

The 2021 stress test exercise aims to assess the resilience of the participants to the adverse scenario(s) by a capital and liquidity perspective

in order to provide supervisors with information on whether these insurers are able to withstand severe but plausible shocks.

While not being a pass/fail exercise, the 2021 exercise has mainly a microprudential approach. It allows EIOPA to make recommendations to the industry and enables supervisors to ask insurance undertakings to take remedial actions, when needed, in order to improve their resilience.

The microprudential assessment is complemented by the estimation of potential spill-over from the insurance sector triggered by widespread reactions to the prescribed shocks.

Scenario

The 2021 stress test exercise focuses on a prolonged COVID-19 scenario in a "lower for longer" interest rate environment.

The scenario, developed in cooperation with the ESRB, elaborates on the ongoing concerns about the possible evolution of the COVID-19 pandemic and its economic ramifications which trigger adverse confidence effects worldwide, and a prolong the economic contraction.

The narrative is translated into a set of market and insurance specific shocks that generate a severe but plausible "double-hit" effect to the insurance industry.

For detailed information on the scenario and on the shocks, see the ESRB Adverse scenario for the EIOPA 2021 Stress Test, the Technical information and in the Technical specifications.

You may visit:
https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-adverse-scenario.pdf

https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-technical-specifications-v1.1.pdf

Approach

The 2021 Stress Test exercise assess the resilience of the European insurance industry by a capital and liquidity perspective:

- the capital assessment relies on the Solvency II framework;

- the liquidity assessment is based on the estimation of the sustainability of the liquidity position.

Participants are requested to estimate their position under two assumptions:

- Fixed balance sheet;
- Constrained balance sheet.

For detailed information on the approach see the Technical Specifications: https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-technical-specifications-v1.1.pdf

Scope

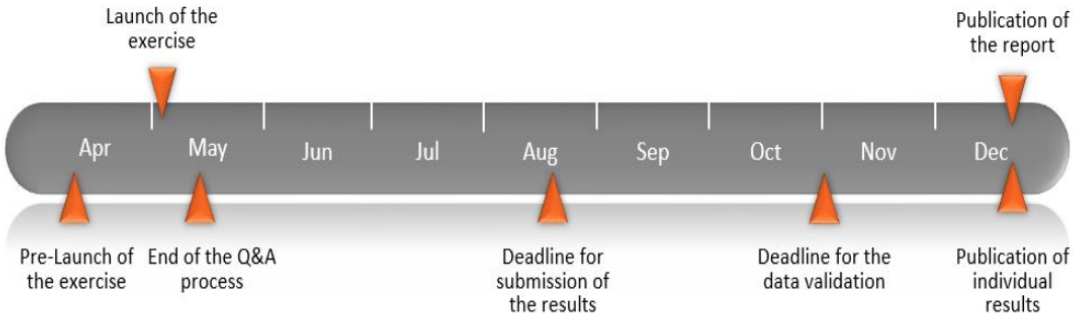
The 2021 exercise targets European (re)insurance groups. The selection of the participating entities is mainly based on size, EU wide market coverage, business lines conducted (life and non-life business) and number of represented jurisdictions.

The local market coverage was taken into account in a second stage.

The target sample defined in cooperation with the National Competent Authorities (NCAs) covers 75% of the EU-wide market based on total assets in the Solvency II.

The list of the undertakings in scope of the 2021 Stress Test exercise is reported in the Technical Specifications.

Working process



To read more: https://www.eiopa.europa.eu/insurance-stress-test-2021_en

Artificial Intelligence Governance Principles: Towards ethical and trustworthy artificial intelligence in the European Insurance sector.

A report from EIOPA´s Consultative Expert Group on Digital Ethics in insurance

Due to technological advances digitalised data and its use play an increasingly important role in our societies.

The amount of digital data doubles in short intervals, it is collected from different sources and formats and its manipulation gets more efficient. Data scientists invent novel ways of drawing better conclusions from the data.

Technology is finally making Artificial Intelligence (AI) into a relevant tool to improve our societies.

Insurance has been a heavy user of data from practically early days of its existence. The collection of data, even when available, has been expensive. Analysis of this data has been expensive too and often inaccurate.

Instead of an as exact as possible knowledge of insured persons and physical objects insurers have had to live with crude indicators of the risk inherent in each case.

The emergence of Big Data (BD) and AI are changing this, making it possible to have more exact knowledge and changing the ways insurers interact with policyholders.

Insurance has also through all of its existence dealt with ethical problems. Fair treatment of the insured pool and each policyholder has created problems that have been solved with varying degrees of success.

Developments with BD and AI are not creating new challenges in this area. Instead, they are offering possibilities to deal with some in a better way but also exacerbating other.

Current ethical issues in insurance are also acute only partly due to changes in BD/AI. Maybe even more often topical issues in this area result from changes in our societies, i.e., from changing thoughts on what a good life is and how individuals should be treated.

Ethics is about good life. There have been different efforts to formalise ethics, i.e., to create a framework to determine in an undisputed manner what is ethical and what is not. This has proved to be impossible. Therefore there cannot be an algorithmic way to integrate ethics into the use of data in a way that always reaches correct solutions.

This report approaches ethical issues in a more down-to-earth manner. Ethics is thought to mean approaches that are fair based on international and national recommendations, standards and treaties, and of course legislation. Our understanding is that this represents what most people would understand as ethical.

Insurance exists in many forms. One dividing line is between (mandatory) social insurance and private insurance. This report concentrates on private insurance. Possible issues on BD/AI in social insurance would need a separate analysis.

Ethical challenges in insurance result from separate interests of the main stakeholders of insurance activity. We can identify three key players:

- an individual seeking insurance cover or being insured,
- the pool of insured risks, and
- the insurer who manages the pool.

Usually the individual in this case is looking for suitable cover at a price that is as low as possible. The pool is a group of risks, independent enough that allows for risk sharing among the group utilising the Law of Large numbers or one of its softer forms. In the interest of the pool there should be certainty that none of its members is taking inappropriate advantage of the pool.

In many cases there are legal, contractual or informal ways of returning a certain part of the profit of the insurer to the pool and its insured even in situations where the insurer is a profit-making entity.

The requirements of insurability and the conflicting interests of these three stakeholders create situations with ethical dilemmas. In many cases this is related to the fair treatment of an individual when the interests of the pool and the insurer are taken into account. One can ask to what extent the legitimate interests of one of these players can be limited in order to honour the legitimate interests of the other two.

In our work we have looked at the challenges to fairness with the emergence of new technologies. Fairness is especially threatened with the treatment of individuals in more or less vulnerable situations. We have outlined tools in transparency and explainability to help identifying areas where fairness is threatened. And we have suggestions on how the

governance of the use of AI should be organised to safeguard sound use of AI.

The scope of our work was ambitious. Analysing how BD/AI influences insurance's many processes and interactions with policyholders was a significant challenge that we took eagerly knowing that compromises in the number of analysed cases would be required.

Some readers may wish that our report had covered specific forms of insurance in greater detail and provided more specific guidance for them.

We believe that, while not covering every possible case, our report provides the tools for individuals and organisations to reflect on the ethical challenges of BD/AI in insurance and apply BD/AI techniques in a trustworthy manner.

Should this require additional specialist knowledge, market participants (consumer associations, insurers and national supervisors) may want to work together in their respective markets to address those specific forms of insurance.

Figure 1 – Examples of AI use cases across the insurance value chain

Product design and development	Pricing and underwriting	Sales and distribution	Customer service	Loss Prevention	Claims management
▪ Historical customer and survey data analysis to inform new products ▪ Predictive modelling of disease development patterns ▪ Novel products, e.g. parametric and usage-based insurance	▪ Enhanced risk assessments combining traditional and new data sources (including IoT data) ▪ Price optimisation: micro-segment / personalised pricing based on non-risk individual behavioural data (e.g. to estimate price elasticity, lifetime value and propensity to churn) and market competition analysis	▪ Digital marketing techniques based on the dynamic analysis of online search behaviour ▪ Virtual Assistant and Chatbots that utilise Natural Language Processing (NLP) and insurance ontologies to support communication ▪ Proactive customer communication, nudging and cross-selling of related services ("next-best action") based on consumer data from Customer Relationship Management (CRM) systems	▪ Call centre sentiment analysis, route cause analysis, dynamic scripting and agent allocation ▪ Customer self-service through multiple channels using NLP, voice recognition, insurance ontology maps and chatbots ▪ Robotic Process Automation (RPA) including Optical Character Recognition (OCR) to extract information from documents (e.g. FNOL, email with questions complaints etc.) and route them to the correct department	▪ Provide diagnostic advice anc coaching based on AI analytics from health and automotive big data, e.g. suggest exercise and driving behaviour changes	▪ Enhanced fraud analytics: claims scoring, anomaly detection, social network analytics and behavioral modelling ▪ Loss reserving: use of AI to estimate the value losses, in particular for high-frequency claims ▪ AI image recognition to estimate repair costs in household property insurance, business premises and automotive ▪ Automated segmentation of claims by type and complexity and automated invoice verification and payment process

Source: EIOPA Consultative Expert Group on Digital Ethics in insurance

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa-ai-governance-principles-june-2021.pdf

Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships

Overview of responses to the public consultation

On 9 November 2020, the Financial Stability Board (FSB) published a discussion paper for public consultation on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships.

The discussion paper drew on findings from a survey conducted among FSB members, and identified a number of issues and challenges.

To facilitate and inform discussions among authorities (including supervisory and resolution authorities), financial institutions and third parties on how to address the issues identified, the discussion paper invited comments from external stakeholders on:

1. the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships (including risks in sub-contractors and the broader supply chain);

2. possible ways to address these challenges and mitigate related risks, including in a cross-border context; and

3. lessons learnt from COVID-19 relating to outsourcing and third-party relationships.

The public consultation period for the discussion paper ended on 8 January 2021. The FSB received 39 responses from a wide range of stakeholders including banks, insurers, asset managers, financial market infrastructures (FMIs), third-party service providers, industry associations, individuals and public authorities.

The FSB also held a virtual outreach meeting in late February 2021 to discuss: evolving industry practices; practical challenges associated with outsourcing and third-party risk management; and potential ways to improve coordination among the relevant stakeholders (i.e. supervisory and resolution authorities, financial institutions and third-party service providers) with a view to enhancing the resilience of financial institutions and the financial system.

Respondents generally welcomed the discussion paper, which they viewed as a timely and balanced overview of the benefits and challenges relating to the evolving nature of financial institutions' outsourcing and third-party dependencies.

Respondents agreed with the challenges and issues identified in the discussion paper, such as: constraints on the rights to access, audit and obtain information from third parties; and concentration risks in the provision of certain critical services that are very difficult to substitute.

In addition, treatment of intra-group outsourcing, fragmentation of regulatory, supervisory and industry practices across sectors and borders, restrictive data localisation requirements, cyber and data security, and resource constrains at financial institutions as well as supervisory authorities were highlighted as potential challenges or issues that deserve attention.

To address these challenges or issues, respondents suggested a range of measures that can be categorised into five areas:

(i) the development of global standards on outsourcing and thirdparty risk management;

(ii) the adoption of consistent definitions and terminology;

(iii) pooled audits, certificates and reports;

(iv) dependency mapping and enhanced supervisory oversight; as well as

(v) enhanced cross-border cooperation and dialogue with stakeholders.

This note summarises the main issues raised and views expressed in the public consultation, including the virtual outreach meeting (which are not necessarily shared and endorsed by FSB members).

To read more: https://www.fsb.org/wp-content/uploads/P140621.pdf

Cyber Security in a changing and complex world

Lindy Cameron, CEO, UK National Cyber Security Centre (NCSC), RUSI Annual Security Lecture

It's great to be back here at RUSI (albeit virtually), at the world's oldest independent defence and security thinktank. It's a real privilege to be giving the second Annual Security Lecture.

And a particular privilege to follow the deeply impressive Dame Cressida Dick, who last year talked about the increasing influence and opportunity of data and technology in modern policing – at a time where a growing proportion of crime in the UK is either digitally enabled or committed entirely online.

We work in close partnership with law enforcement, so it won't surprise you that my lecture today will also look at cyber threats and opportunities. But I also look forward with hope to the day soon when it's unremarkable to have two senior women giving a lecture on national security. We're on our way but not there yet.

I'm also very proud to be here as the second head of the National Cyber Security Centre, which after only five years plays a key role in the UK's national security.

Its creation in 2016 showed real foresight and is widely recognised as an example others want to emulate – a partnership of government, law enforcement, intelligence and the private sector. And we have achieved a huge amount since then.

We have dealt with over 2,000 significant incidents.

We have protected the UK at scale through Active Cyber Defence – taking down more than 700,000 online scams in the last year alone, 80,000 of which were new tip offs from the British public through the hugely successful Suspicious Email Reporting Service.

We have raised resilience in all sectors of our critical national infrastructure, and built coalitions with businesses, charities and education to develop accessible and actionable cyber security tools and advice.

Over 55,000 teenagers have participated in the CyberFirst Girls competition and our cyber security courses.

And we have made the internet safer and easier to use for UK citizens through our Cyber Aware campaign, challenging password culture and victim blaming.

So I'm not sure if you planned it like this, but this feels like a really important moment to be talking about cyber security - and about cyber security as an international and not just a national issue, as an issue of mainstream national security policy.

As the Attorney General said in his landmark 2018 Chatham House speech on international law in this area, the influence of cyberspace on international relations is 'growing not shrinking.'

Of course the UK has seen cyber security as a mainstream national security issue for some time, key to our strategy, statecraft and the expression of our national values.

This was clear in the 2016 Cyber Security Strategy, which drove institutional change and investment. But the recent Integrated Review of Security, Defence, Development and Foreign Policy was even clearer on the importance of cyberspace in protecting our core interests of sovereignty, security and prosperity.

It outlined a vision of the UK, more robustly resilient to the threats of a competitive world, but also better able to take advantage of its opportunities, and working with allies to shape that world for the benefit of all.

Don't just search for the 'cyber' section of the integrated review – stand back and understand how fundamental the ability to operate in cyberspace is to the whole vision, underpinned by investment in the UK as a global science and technology and responsible cyber power.

You will have heard key interventions by the Foreign Secretary and Home Secretary last month at the NCSC's flagship CYBERUK conference – livestreamed on YouTube – and still available – and seen many interventions just in the last week from the Foreign Secretary, Defence Secretary and alumni of the national security community.

What is changing is that the international consensus on this is building. You can see that today as NATO leaders meet to agree how to adapt further to cyber challenges and how to strengthen the resilience of the alliance, in

the language used by leaders at the G7 summit at Carbis Bay in Cornwall, and in the prospect of a G7 Future Tech Forum.

The G7 and like minded partners are both calling out cyber threats and promising to work together on cyber opportunities like future technical standards that are in line with our core values.

This is particularly true of the incoming Biden administration, one of whose very first national security challenges was the response to the SolarWinds intrusion, and who in recent days have, in the words of Deputy National Security Adviser Anne Neuberger 'stepped up' their response to ransomware in the face of live examples of the cyber threat to critical national infrastructure like the Colonial Pipeline, issuing a wide ranging cyber Executive Order.

We have seen the nomination of influential experts like Chris Inglis, author of the Cyberspace Solarium Commission report, and Jen Easterley, to key positions in the new administration. And a recognition that cyber security requires the same kind of joined up, nationally coordinated whole of government response as counter terrorism – although the threats are very different.

So there is a moment now, to take our alliances in this space to a different level. And we in the UK are well positioned to play a key leading role in this. One of our strengths, in my view, is that we consistently treat cyber security not just as a national security issue but as a mainstream public policy issue, where – for example – success in the education sector is as important as more traditional national security concerns.

The UK's Integrated Review is really clear on this: it talks about "pursuing a whole of nation effort, bringing together industry and academia in partnership" and "engaging citizens, who have a central role to plan in our national security".

I see our other key strength as the centrality of resilience in our strategy – recognising that we need to 'make the UK the safest place to live and work online' for everyone – citizens and businesses as much as government.

That is not to say we are perfect – as I have said before, there is no room for complacency, and we have much more to do. But we know our approach works, and we should bring others with us on this journey.

So it is very prescient and rather timely of you here at RUSI to choose this issue for your second annual Security Lecture. And thank you for choosing me.

Those of you who know me and my background – and of course I'm not unfamiliar with RUSI and its members – will know that my entire career has been about a 'whole of nation' approach, whether at home or internationally.

So I hope that, despite being an illustrious security and defence thinktank, you are not expecting me to see cyberspace purely as a war zone, or my lecture to be filled with gory battlefield imagery.

Others can do that far better than me. My career in national security has always been about the messy reality of people's everyday lives and the transformative potential of economic growth, even in conflict.

And that's why, as you can imagine, when I look at cyberspace, I don't see the threat as being confined to state actors. That is not in any way to underestimate the scale or seriousness of state activity or data theft.

It consumes a very significant part of my team's most sophisticated capability. State sponsored cyber activity represents one of the most malicious strategic threats to the UK's national interests.

It is hugely important. Tracking and defending the UK from our most sophisticated adversaries represents much of our core business, usually working to support victims behind the scenes.

But it is not the only threat. And if we treated it as such, we would misrepresent the totality of the challenge and run the risk of an inappropriate response.

Firstly because we all know that looking at a conflict solely through the lens of the protagonists would be to miss the inevitable opportunistic criminals exploiting the black market. And secondly because cyberspace is – primarily - a peaceful domain, of prosperity and opportunity. And that should tell us something profound about what we need to protect: the aggregation of economic harm to individuals and organisations.

The UK digital sector employed 1.5m people and added £150bn to the UK economy in 2019. And that's true not only in the UK, but internationally.

And of course – as this audience will be well aware - state actors are a reality in cyberspace. Four nation states – China, Russia, North Korea and Iran, have been a constant presence in recent years. And as I've said before, we face a determined, aggressive Russia, seeking traditional political advantage by new, high-tech means.

We live in a business and corporate environment where Chinese cyber attacks on our commercial interests are something our companies treat as business as usual.

And authoritarian regimes including North Korea and Iran use digital technology to sabotage and steal.

This is not a surprise, and it's not new. Of course, you as a think tank will know this. A recent NCSC assessment of the Threat to Think Tanks noted it is 'almost certain' that the primary cyber threat to UK think tanks is from nation state espionage groups and it is 'highly likely' that they will seek to gain strategic insights into government policy, trade agreements and commercially sensitive information. So it's not just governments that are at risk.

But it's no longer 'just' espionage and data theft that is a threat. Even where it is, the complexity of modern supply chains may mean that many others can be caught in the crossfire and suffer compromises to their systems, as we saw with the recent SolarWinds Orion compromise and subsequent targeting, attributed as being 'highly likely' the work of the Russian intelligence services.

So although the threat has grown, our investment in cyber security means we know more about these threats now than we did five years ago when the NCSC was set up. And our world leading systems for sharing information with trusted partners means we can use this to improve the resilience of businesses and civil society, not just government and critical national infrastructure. Our ability to do this is the envy of many.

We have also used this knowledge to contribute to a series of public attributions that have exposed state activity -including attributing Not Petya and the DNC hack to Russia; the APT10 intrusion set to China; Wannacry to the North Korean Lazarus Group and the Mabna Institute to Iranian actors.

Attribution is part of our approach to cyber deterrence, as previous Foreign Secretaries have laid out. We seek to discover who is behind activity; expose the detail of their action in a way which helps both public and private sector defend; prosecute where possible, and – when we choose to – respond.

Because although building cyber resilience is crucial, the government also needs the capability to take action directly to counter a range of threats – a 'whole of cyber' approach. And that's why one of the range of strategic outcomes supported by the new National Cyber Force's cyber operations is cyber security, working in close partnership with us at NCSC.

So what I find most worrying isn't the activity of state actors. Nor is it an improbable cyber armageddon – though if you want a good description of a sort of dystopian, Blade Runner style future, check the attention-grabbing opening pages of the Solarium report.

What I worry most about is the cumulative effect of a potential failure to manage cyber risk and the failure to take the threat of cyber criminality seriously.

For the vast majority of UK citizens and businesses, and indeed for the vast majority of critical national infrastructure providers and government service providers, the primary threat is not state actors but cyber criminals, and in particular the threat of ransomware.

This has become more evident than ever during covid – that we need to focus on victims not just threat, and that small harms can amount to a cumulative risk of national significance.

This is the most insidious cyber security risk – not the threat from, but threat to; and not the loss of data but the impact on operations, large and small, that stops people and business from being able to live their day to day lives.

The sheer volume makes it the most impactful threat we face. We have seen it affect the NHS with WannaCry, prevent students accessing classes in the last few weeks, and shut down local authorities at great cost to the public purse, meaning the public cannot access services, pay their bills or, in some cases, even buy a house.

Ransomware has historically been the preserve of high-end cyber crime groups with access to advanced technical skills and capabilities based in overseas jurisdictions who turn a blind eye or otherwise fail to act to pursue these groups.

But the ecosystem is evolving through what we call Ransomware as a Service, (RaaS) and the 'As a Service' business model where ransomware variants and commodity listings, such as lists of credentials, are available off the shelf for a one-off payment or a share of the profits.

We know that there are campaigns to recruit new affiliates. As a result, users buy from developers without the costs and risks of developing it themselves, and that enables actors less experienced in ransomware to acquire tools to conduct their own attacks.

As the business model has become more and more successful, with these groups securing significant ransom payments from large and profitable

businesses who cannot afford to lose their data to encryption or to suffer the down time while their services are offline, the market for ransomware has become increasingly 'professional'.

If your files are encrypted by ransomware you may be offered the services of a 24/7 help centre to quickly pay the ransom and get yourself back online. The ransom note accompanying the attack gives you the contact details to use to negotiate with the attackers and unlock your files. Everything is geared to make it as easy as possible to simply pay the ransom and move on.

High end crime groups spend time conducting in depth reconnaissance on their targeted victims. They will identify your cyber security weaknesses that they can exploit. They will use spoofing and spearphishing to masquerade as internal employees to get access to all of the networks they need.

They will look for the business-critical files to encrypt and hold hostage. They may identify embarrassing or business sensitive material that they can threaten to leak or sell to others. And they may even research your cyber insurance policy to see if you are covered to pay ransoms.

This process can be painstaking and lengthy, but it means that, when they are ready to deploy, the effect of ransomware on an unprepared business is brutal. Everything is taken out. Files are encrypted. Servers go down. Digital phonelines no longer function. Everything comes to a halt and your business stops in its tracks.

Some of the most powerful testimonies I've heard since starting this job have been from chief executives faced with a ransomware attack they were under-prepared for.

We support victims of ransomware every day, but turning up to a ransomware incident as the NCSC feels like the fire service turning up to a house that has already burned down. There might be some forensic evidence that the police might pursue.

Occasionally (but less so over time) there might be a flaw in the malware or its deployment that we can make the most of. Even more rarely, we just might be able to get a decryption key. But these groups know what they're doing, and that hardly ever happens. More often than not, it's a case of rebuilding from scratch and restoring the data – assuming you have – and please read the advice – an offline backup that can be used for this.

But it doesn't stop there. Over the last year or so these cyber crime groups have evolved their techniques to include data extortion. Even if you have

offline backups and can get back on your feet without paying a ransom, the group will threaten to leak the data they have stolen.

This can make all your business information, personal sensitive data, otherwise embarrassing content, available online for all to see. So, this is now the double whammy of ransomware; even if you have good data storage in place they can still try and hold you to ransom.

Many victim organisations in this situation feel they have no choice but to pay. It's the same emotional blackmail technique that con-artists play on vulnerable elderly people they are trying to extract bank details from.

I have huge sympathy for how that must feel. But paying a ransom in no way guarantees the return of data (which unlike a human kidnap victim, can be copied). And it funds a criminal enterprise which will be encouraged to try the same thing on others.

This isn't a counsel of despair. In some respects, our response to ransomware is straightforward: we need to continue to build the UK's cyber resilience so that attacks cannot reach their targets in the first place. We have great advice on how to do this with our 10 Steps to Cyber Security and we've made huge strides across a range of sectors.

And it's about preparing, planning and exercising, all the way up to Board level, working on the assumption that a cyber criminal will be as interested in your weaknesses as a burglar is in your open window.

Reporting really matters – even if you are a victim and it's too late to limit the damage to your business, it helps us help others. All this not only helps make businesses resilient to ransomware, but to the full range of cyber threats they face, and deters adversaries by increasing the cost of an attack.

But in many other respects it requires a whole of government response. This starts with the efforts to prevent the activities of the groups behind these damaging attacks. These criminals don't exist in a vacuum.

They are often enabled and facilitated by states acting with impunity. International and diplomatic efforts need to be coordinated to stop them. And it includes seeking the strongest criminal justice outcomes for those we apprehend.

There are other players with a key role such as the cyber insurance industry which has a role to play in bearing down on the payment of ransoms and cryptocurrency entities who facilitate suspicious transactions.

There will also be a role for cyber operations, taking direct action alongside law enforcement; disrupting cyber crime marketplaces where criminals buy and sell credentials, and disrupting ransomware groups.

None of this is a substitute for effective cyber security, but it is an increasingly necessary part of the national toolkit and a whole of nation approach. And that national approach must be coordinated with others, as the Foreign Secretary outlined in his interview with the Telegraph last week, and indeed as the G7 communique lays out.

A coordinated response on ransomware, involving these key players, would have the added benefit of helping us meet broader national and strategic international objectives, making the UK a more resilient and prosperous place to live and do business online.

And it's vital we recognise this - because we are at inflection point in global technology. Jeremy Fleming, Director of GCHQ, described a 'moment of reckoning' recently, where without action the key technologies we rely on won't be shaped or controlled by the likeminded democracies.

We already know proliferation is a risk. We know there are companies that sell high end state-like capabilities that exploit computer networks and at the other end of the spectrum, you can buy an 8 radio SIMBox for $300 which allows you to send thousands of cyber crime SMS campaigns every hour. These things won't just matter to UK customers, they matter globally.

But we also know that in every era of the internet we have struggled to anticipate the magnitude or speed of change ahead of us. Back in the 1980s when I was loading computer games onto my ZX Spectrum+ using a cassette recorder I couldn't have imagined a mobile phone, let alone an Apple Watch.

So that's why the UK is leading the way in anticipating the potential scale of change in the future. And as I said, this needs to be a whole of nation approach. Let me give you three examples where government can play a role.

Firstly, the Internet of Things. On Consumer IoT devices, we have developed a cyber security standard now embedded in draft legislation that products sold in the UK will have to meet. That has become a European, and we hope, a global standard. We want to see the same radical change in assumptions about the security of internet connected devices as we've seen in car safety for baby seats over the last decades.

Secondly, the new Telecoms (Security) Bill will see a regulatory framework place security requirements on how telecoms operators build and run their

networks. No one has taken it to this level before - it will create the toughest telecoms security regime in the world.

It will provide new legal powers in two parts: a new security regime with a range of new security duties on operators and new monitoring and enforcement powers for Ofcom. And new national security powers, replacing the thus far voluntary arrangement between the government and operators, to remove and restrict use of goods, services, and equipment from vendors designated as high risk. Non-compliance could result in fines of up to 10% of turnover or a daily penalty of £100,000.

The National Security and Investment Act, the biggest shake-up of the UK's investment screening regime in 20 years, will modernise government's powers to investigate and intervene in potentially hostile foreign direct investment, while advancing the UK's world-leading reputation as an attractive place to invest.

Of the 17 sectors it covers, those most important for cyber security (and where we were instrumental in developing the definitions) are Artificial Intelligence, computing hardware, data infrastructure, communications, quantum technologies and crypt authentication.

That helps us protect our critical services from cyber-attacks and improve the underlying security of the Internet through technological improvement.

But government cannot do this alone. We will continue to take a whole-of-society approach to improving the cyber resilience of the UK: industry, academia, and civil society all have a role to play.

While government is uniquely able to disrupt and deter our adversaries, it is network defenders in industry, and the steps that all organisations and citizens are taking that are protecting the UK from attacks, day in, day out. The protection they provide is crucial to the digital transformation of the economy, and every organisation, large and small, has a role to play.

We have come a long way, but there is room for improvement, and for even deeper collaboration. I hope the review of the Computer Misuse Act announced by the Home Secretary will help with this.

Yet collaboration cannot end at our borders; UK cyber resilience is not just a UK challenge. This is a global challenge and we cannot do this alone. We must continue to deepen our partnerships with partners around the world to support of our mutual resilience, both in response to the immediate ransomware threat but also to the longer term benefit of all of our economies and societies.

It's fantastic to see the consensus building that cyber security is a leader-level national security issue, as we have done in the last few days at the G7 and Nato. There is probably a whole other speech to give on what more we can do to build on that consensus and momentum, which I don't have time to do full justice to today. But in summary, I think what we can do is to:

Firstly, agree what's acceptable. As the G7 communique flags we need to work together to further a common understanding of how international law applies to cyberspace. We need to do the work as a global community to clarify and develop rules that are right for the digital age and the Foreign Secretary has made clear the UK plans to lead on this.

I therefore welcome the UN Government Group of Experts on cyberspace reaching its first agreement since 2015, building on the global appetite for clear appetite for progress captured in the consensus report by the Open Ended Working Group earlier this year.

Secondly, we need to set standards more effectively. Whatever model of standards body we are talking about – government led, industry only or genuinely multistakeholder - they are critical to the future of technology, including interoperability and security.

The UK prefers multi-stakeholder bodies because that brings balance. This is not about government control – this is about upping our engagement in a way that will benefit our prosperity and security and uphold our values.

And thirdly we need to build alliances. We already have fantastic partnerships with our 5 eyes allies and through NATO. Based on trust, collective action and a shared vision for the future.

But for a whole of nation partnership approach and to deal with the challenges of cyber security in a rapidly changing world, we must also deepen our partnerships with like-minded European countries, partners in Asia and beyond.

So in conclusion:

This really does feel like the moment when the world starts to take cyber security seriously, as a national security issue and a public policy issue.

As I have been clear, I see cyberspace primarily as a domain of civic and commercial interaction that enables economic growth and wider societal benefits, and that must remain free, open, peaceful and secure.

It is a real moment of opportunity, despite the current focus on threats.

And for the UK, it is also a moment of leadership. We are ahead of the game – we have invested in cyber security and set ourselves up for success. We have a whole of nation strategy with resilience at its core and we must deliver on that.

And with our new cyber strategy this year, we will have a chance to lay out how we see the future in more detail. I look forward to NCSC playing our part in that future.

Yoy may visit: https://www.ncsc.gov.uk/speech/rusi-lecture

A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime

EU Serious and Organised Crime Threat Assessment (SOCTA)

The EU Serious and Organised Crime Threat Assessment (SOCTA) is the product of systematic and comprehensive analysis of law enforcement information on criminal activities and networks affecting the EU.

The SOCTA is designed to assist decision-makers in the prioritisation of serious and organised crime threats.

It has been produced by Europol, drawing on extensive contributions from the organisation's databases and external partners. Europol would like to express its gratitude to Member States, non-EU countries, EU agencies and institutions and international organisations for their valuable contributions and input.

The EU SOCTA 2021 is the outcome of a detailed analysis of the threat of serious and organised crime facing the EU, providing information for practitioners, decision-makers and the wider public. As a threat assessment, the SOCTA is a forward-looking document that assesses shifts in the serious and organised crime landscape.

The SOCTA 2021 sets out current and anticipated developments across the spectrum of serious and organised crime, identifies the key criminal groups and individuals involved in criminal activities across the EU and describes the factors in the wider environment that shape serious and organised crime in the EU.

The SOCTA 2021 provides an overview of the current state of knowledge on criminal networks and their operations based on data provided to Europol by Member States and partners and data collected specifically for the SOCTA 2021.

In trying to overcome the established, and limiting, conceptualisation of organised crime groups, this assessment focuses on the roles of criminals within criminal processes and outlines how a better understanding of those roles allows for a more targeted operational approach in the fight against serious and organised crime.

- Close to 40% of the criminal networks active in the EU are involved in the trade in illegal drugs.

- Around 60 % of the criminal networks active in the EU use violence as part of their criminal businesses.

- The use of corruption and the abuse of legal business structures are key features of serious and organised crime in Europe. Two thirds of criminals use corruption on a regular basis. More than 80 % of the criminal networks use legal business structures

Similar to a business environment, the core of a criminal network is composed of managerial layers and field operators. This core is surrounded by a range of actors linked to the crime infrastructure providing support services, such as brokers, document fraudsters, technical experts, legal and financial advisors, money launderers and other service providers.

A key characteristic of criminal networks, once more confirmed by the pandemic, is their agility in adapting to and capitalising on changes in the environment in which they operate. Obstacles become criminal opportunities and may be as simple as adapting the narrative of a known modus operandi.

The use of violence by criminals involved in serious and organised crime in the EU appears to have been increasing in terms of the frequency of use and its severity. Criminals use violence indiscriminately and target victims without regard for their involvement or standing, often accepting harm to innocent bystanders. The threat from violent incidents has been augmented by the frequent use of firearms or explosives in public.

Corruption is a feature of most, if not all, criminal activities in the EU. Corruption takes place at all levels of society and can range from petty bribery to complex multi-million-euro corruption schemes. Corruption erodes the rule of law, weakens institutions of states and hinders economic development. Corruption is a key threat to be addressed in the fight against serious and organised crime. Almost 60 % of the criminal groups reported for the SOCTA 2021 engage in corruption[2].

The scale and complexity of money laundering activities in the EU have previously been underestimated. Serious and organised crime in the EU fundamentally relies on the ability to launder vast amounts of criminal profits. For this purpose, professional money launderers have established a parallel underground financial system to process transactions and payments isolated from any oversight mechanisms governing the legal financial system. This parallel system ensures that the criminal proceeds cannot be traced as part of a sophisticated criminal economy.

Legal business structures such as companies or other entities are used to facilitate virtually all types of criminal activity with an impact on the EU. Criminals directly control or infiltrate legal business structures in order to facilitate their criminal activities. All types of legal businesses are potentially vulnerable to exploitation by serious and organised crime. More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities. About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level.

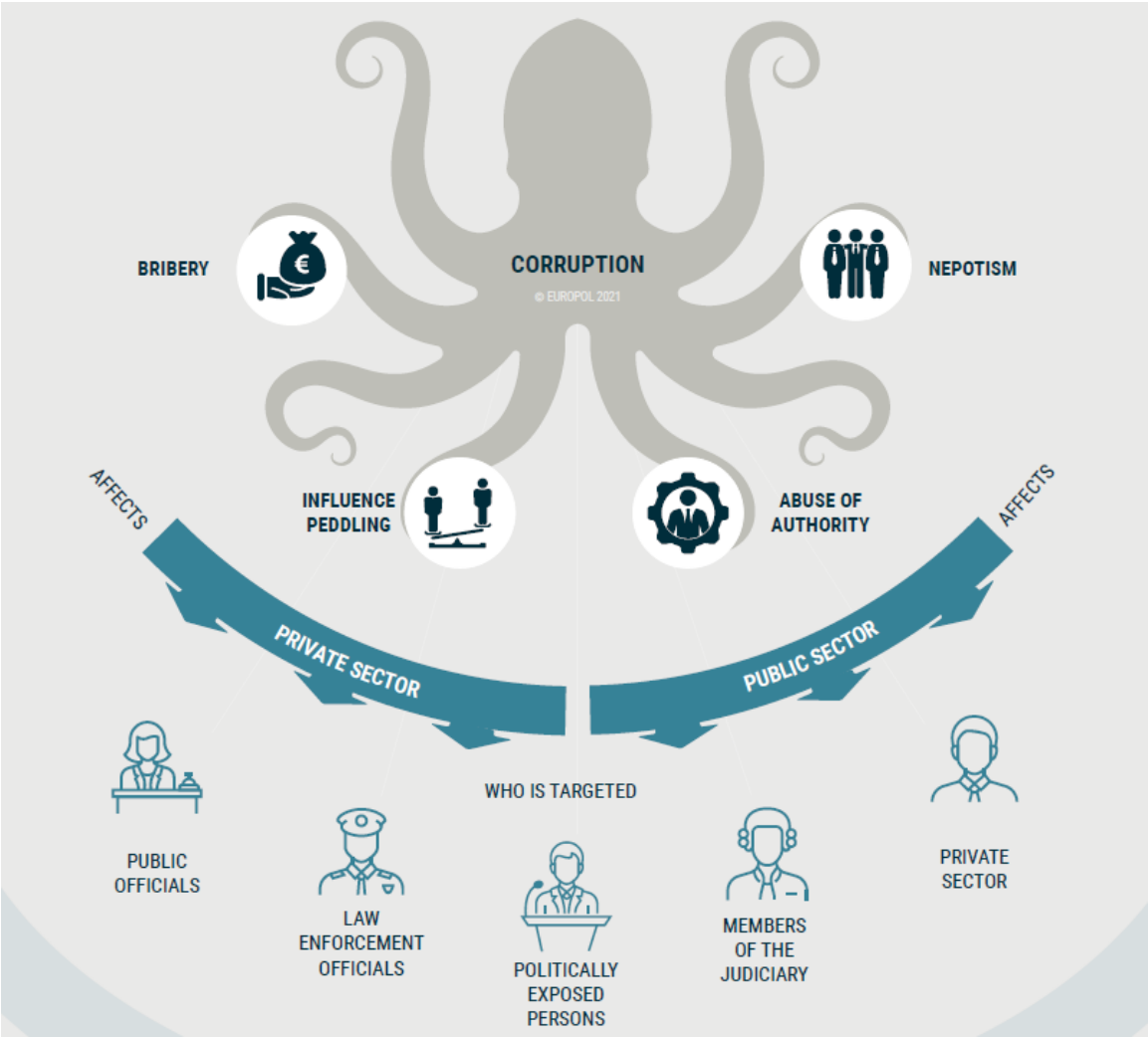
The use of technology is a key feature of serious and organised crime in 2021. Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods or to spread disinformation. The online environment and online trade provide criminals access to expertise and sophisticated tools enabling criminal activities.

A potential deep economic recession following the COVID-19 pandemic will fundamentally shape serious and organised crime in the EU for the near future. Previous periods of economic stress can provide some degree of insight into how these developments might affect crime in the EU and what responses need to be formulated to counter existing and emerging threats to the EU's internal security during this time.

The threat from **cyber-dependent crime** has been increasing over the last years, not only in terms of the number of attacks reported but also in terms of the sophistication of attacks. Cyber-dependent crime is likely significantly underreported. The rapidly progressing digitalisation of society and the economy constantly creates new opportunities for criminals involved in cyber-dependent crime. Fraud schemes take advantage of the digital era. Online fraud schemes target private individuals, businesses and public sector organisations.

The COVID-19 pandemic has had a significant impact on the serious and organised crime landscape in the EU. Criminals were quick to adapt illegal products, modi operandi and narratives in order to exploit the fear and anxieties of Europeans and to capitalise on the scarcity of some vital goods during the pandemic. While some criminal activities will or have returned to their pre-pandemic state, others will be fundamentally changed by the COVID-19 pandemic.

Serious and organised crime deeply affects all layers of society; in addition to the direct impact on the daily lives of EU citizens, it also undermines the economy, state institutions and the rule of law.



To read more: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Central bank digital currencies (CBDCs): an opportunity for the monetary system

Key takeaways

• Central bank digital currencies (CBDCs) offer in digital form the unique advantages of central bank money: settlement finality, liquidity and integrity. They are an advanced representation of money for the digital economy.

• Digital money should be designed with the public interest in mind. Like the latest generation of instant retail payment systems, retail CBDCs could ensure open payment platforms and a competitive level playing field that is conducive to innovation.

• The ultimate benefits of adopting a new payment technology will depend on the competitive structure of the underlying payment system and data governance arrangements. The same technology that can encourage a virtuous circle of greater access, lower costs and better services might equally induce a vicious circle of data silos, market power and anti-competitive practices. CBDCs and open platforms are the most conducive to a virtuous circle.

• CBDCs built on digital identification could improve cross-border payments, and limit the risks of currency substitution. Multi-CBDC arrangements could surmount the hurdles of sharing digital IDs across borders, but will require international cooperation.

Introduction

Digital innovation has wrought far-reaching changes in all sectors of the economy. Alongside a broader trend towards greater digitalisation, a wave of innovation in consumer payments has placed money and payment services at the vanguard of this development.

An essential by-product of the digital economy is the huge volume of personal data that are collected and processed as an input into business activity.

This raises issues of data governance, consumer protection and anticompetitive practices arising from data silos.
This chapter examines how central bank digital currencies (CBDCs) can contribute to an open, safe and competitive monetary system that supports innovation and serves the public interest.

CBDCs are a form of digital money, denominated in the national unit of account, which is a direct liability of the central bank.

CBDCs can be designed for use either among financial intermediaries only (ie wholesale CBDCs), or by the wider economy (ie retail CBDCs).

The chapter sets out the unique features of CBDCs, asking what their issuance would mean for users, financial intermediaries, central banks and the international monetary system.

It presents the design choices and the associated implications for data governance and privacy in the digital economy.

The chapter also outlines how CBDCs compare with the latest generation of retail fast payment systems (FPS, see glossary).

To set the stage, the first section discusses the public interest case for digital money.

The second section lays out the unique properties of CBDCs as an advanced representation of central bank money, focusing on their role as a means of payment and comparing them with cash and the latest generation of retail FPS.

The third section discusses the appropriate division of labour between the central bank and the private sector in payments and financial intermediation, and the associated CBDC design considerations.

The fourth section explores the principles behind design choices on digital identification and user privacy.

The fifth section discusses the international dimension of CBDCs, including the opportunities for improving cross-border payments and the role of international cooperation.

Money in the digital era

Throughout the long arc of history, money and its institutional foundations have evolved in parallel with the technology available. Many recent payment innovations have built on improvements to underlying infrastructures that have been many years in the making.

Central banks around the world have instituted real-time gross settlement (RTGS) systems over the past decades.

A growing number of jurisdictions (over 55 at the time of writing) have introduced retail FPS, which allow instant settlement of payments between households and businesses around the clock.

FPS also support a vibrant ecosystem of private bank and non-bank payment service providers (PSPs, see glossary).

Examples of FPS include TIPS in the euro area, the Unified Payments Interface (UPI) in India, PIX in Brazil, CoDi in Mexico and the FedNow proposal in the United States, among many others.

These developments show how innovation can thrive on the basis of sound money provided by central banks.

Yet further-reaching changes to the existing monetary system are burgeoning.

Demands on retail payments are changing, with fewer cash transactions and a shift towards digital payments, in particular since the start of the Covid-19 pandemic.

In addition to incremental improvements, many central banks are actively engaged in work on CBDCs as an advanced representation of central bank money for the digital economy.

CBDCs may give further impetus to innovations that promote the efficiency, convenience and safety of the payment system.

While CBDC projects and pilots have been under way since 2014, efforts have recently shifted into higher gear.

The overriding criterion when evaluating a change to something as central as the monetary system should be whether it serves the public interest.

Here, the public interest should be taken broadly to encompass not only the economic benefits flowing from a competitive market structure, but also the quality of governance arrangements and basic rights, such as the right to data privacy.

It is in this context that the exploration of CBDCs provides an opportunity to review and reaffirm the public interest case for digital money.

The monetary system is a public good that permeates people’s everyday lives and underpins the economy.

Technological development in money and payments could bring wide benefits, but the ultimate consequences for the well-being of individuals in society depend on the market structure and governance arrangements that underpin it.

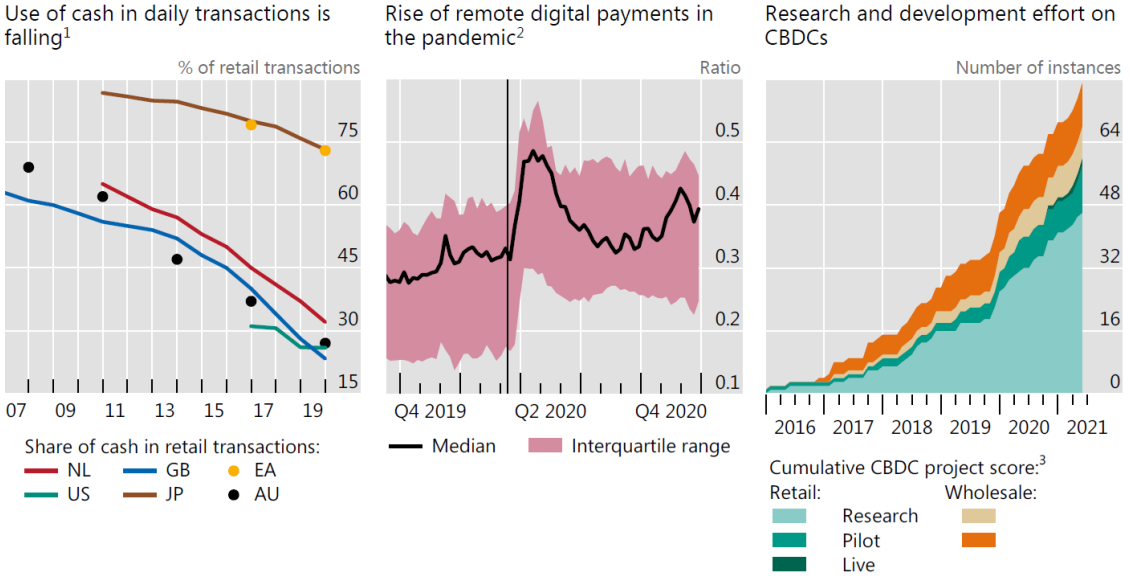
The same technology could encourage either a virtuous circle of equal access, greater competition and innovation, or it could foment a vicious circle of entrenched market power and data concentration.

The outcome will depend on the rules governing the payment system and whether these will result in open payment platforms and a competitive level playing field.

Central bank interest in CBDCs comes at a critical time. Several recent developments have placed a number of potential innovations involving digital currencies high on the agenda.

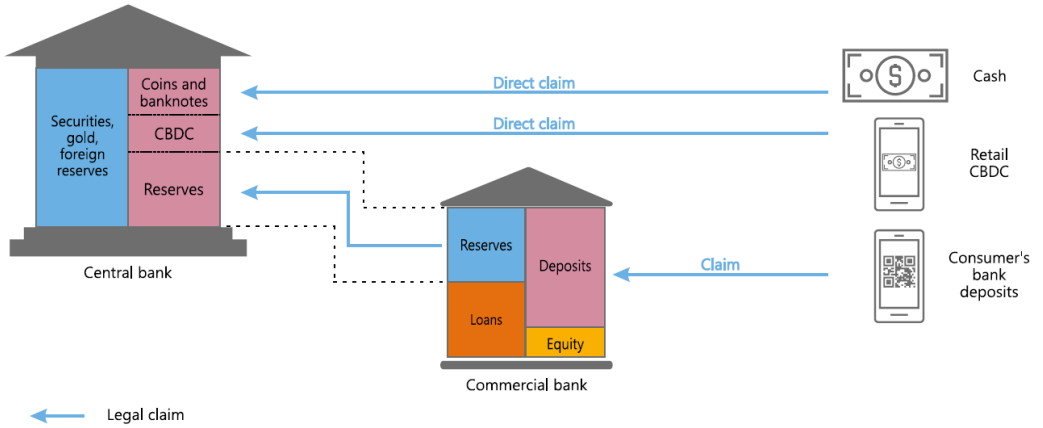
To read more: https://www.bis.org/publ/arpdf/ar2021e3.pdf

As cash use falls and digital payments rise, CBDC projects are moving ahead — Graph III.1



The monetary system with a retail CBDC

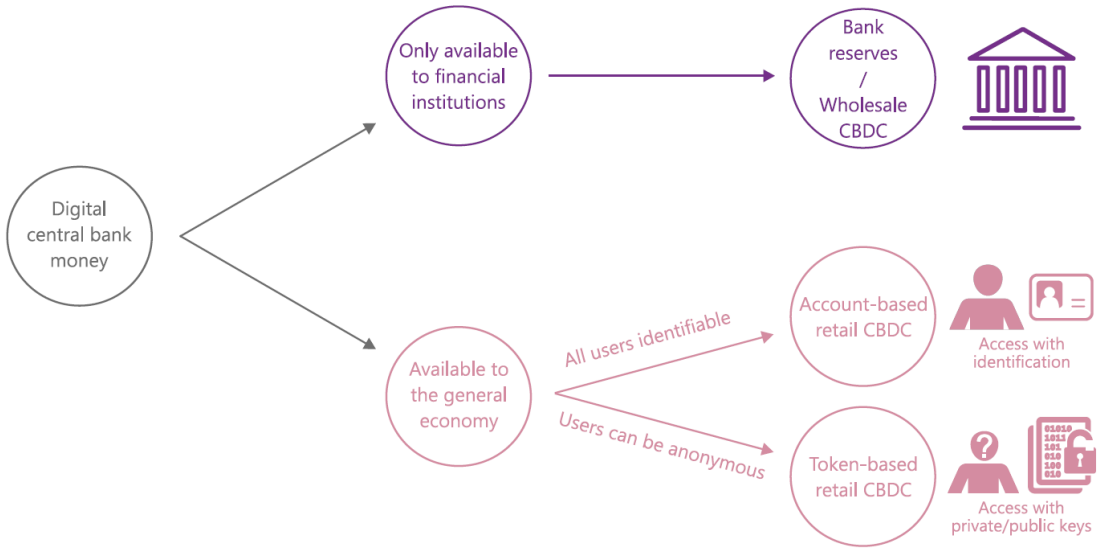
Graph III.4



Source: R Auer and R Böhme, "Central bank digital currency: the quest for minimally invasive technology", *BIS Working Papers*, no 948, June 2021.

Forms of digital central bank money

Graph III.5



Prepared remarks at London City Week

SEC Chair Gary Gensler

Thank you for that kind introduction, Anthony. As is customary, I'd like to note that I'm not speaking on behalf of my fellow Commissioners or the SEC staff.

I'm honored to be speaking again at London City Week. It's been eight years since I last spoke here. That was about benchmark interest rates and the London Interbank Offered Rate (LIBOR).

I may come back to that, but I'm mostly going to take the opportunity to discuss three key areas of the reform agenda at the Securities and Exchange Commission.

The SEC was set up in the 1930s by Franklin Delano Roosevelt and the U.S. Congress to look after working families' savings in the depths of the Great Depression.

Congress passed a number of laws with the same basic ideas — among them, that investors get to decide what risks they wish to take, as long as companies provide appropriate disclosures; that working families should be protected with regard to their investment advisers; and that the stock exchanges themselves should be free of fraud and manipulation.

Those protections put in place by Congress and the early SEC have stood the test of time. I think they're a large part of our economic success — why the U.S. has the largest, most vibrant capital markets in the world.

We can't rest on our laurels, though. Technology is always changing the face of finance. Technology and finance have coexisted in a symbiotic relationship since antiquity. That was true long ago of the invention of money; it's true today of mobile brokerage apps, robo-advising, and artificial intelligence.

But our core principles stay the same: protecting investors, facilitating capital formation for individuals and companies, and maintaining fair, orderly, and efficient markets between them.
As the new Administration has gotten underway in the United States, we at the SEC have recently published a new regulatory agenda. It covers a lot of

ground: investment fund rules, insider trading, shareholder democracy, special purpose acquisition companies, and much more.

Today, I won't cover the nearly 50 items on the agenda. Instead, I'm going to focus on three broad areas: public company disclosure, market structure, and transparency initiatives.

Public Company Disclosure

First, I've asked staff to put together recommendations on mandatory company disclosures on climate risk and on human capital.

Today, investors increasingly want to understand the climate risks of issuers. Investors representing literally tens of trillions of dollars of assets under management are looking for consistent, comparable, decision-useful information to determine whether to invest, sell, or make a proxy vote one way or another.

I've asked staff for recommendations for our consideration around governance, strategy, and risk management related to climate risk. In addition, staff are looking into a range of specific metrics, such as greenhouse gas emissions, to determine which are most relevant to investors in our markets.

Further, I've asked staff to consider potential requirements for companies that have made forward-looking climate commitments, or that have significant operations in jurisdictions with national requirements to achieve specific, climate-related targets.

We just received at the SEC more than 400 unique comment letters on these subjects in a public statement released by my fellow Commissioner Allison Herren Lee. Many comments referenced the work of various groups, such as the Task Force on Climate-related Financial Disclosures (TCFD).

I'm really struck by the call for enhanced disclosures.

I've also asked staff to consider the ways that funds are marketing themselves to investors as sustainable, green, and "ESG," and what factors undergird those claims.

Further, investors have said that they want to better understand one of the most critical assets of a company: its people. To that end, I've asked staff to propose recommendations for the Commission's consideration on human capital disclosure.

This builds on past agency work and could include a number of metrics, such as workforce turnover, skills and development training, compensation, benefits, workforce demographics including diversity, and health and safety.

Disclosure helps companies raise money. It helps the efficient allocation of capital across the market. And it helps investors place their money in the companies that fit their investing needs.

Market Structure

Next, let me turn to market structure. At the SEC, we oversee the nearly $45-trillion public equity markets and the $50-trillion fixed income markets, including Treasury markets, corporate bonds, municipal bonds, and more.

I've asked staff to consider the impact that technology has made in every one of these markets, and how we can ensure that we bring the greatest competition and efficiency to those markets — for investors and issuers.

In 1998, after the internet came along, the SEC stood-up new rules for alternative trading systems to govern equity trading off of traditional exchanges.

The SEC continued to update equity market rules in 2005, stitching together a framework for both on- and off-exchange trading. I've asked the staff to take a broader look at how we might update our rules for the current technologies and business models in the equity markets.

For example, I've asked SEC staff to consider the practice known as payment for order flow. We've seen a notable rise in payment for order flow in the U.S., something that you've banned in the United Kingdom.

Canada and Australia also don't allow broker-dealers to route retail orders to wholesalers in return for payments. The European Securities and Markets Authority has raised concerns about these potential conflicts of interest between payment for order flow and best execution.

Today, our markets essentially have three different segments. While the public generally thinks of lit markets when they think of buying or selling equities — markets like Nasdaq and the New York Stock Exchange — those big public exchanges only accounted for about 53 percent of trading volume in January.

So where's the other 47 percent — trading interest that's not displayed on the lit markets? It's executed by alternative trading systems, which include

dark pools, and by off-exchange wholesalers. Thus, significant trading interest on these platforms is not necessarily being reflected in the commonly cited National Best Bid and Offer quote.

I've asked staff to consider whether this equity market structure, as currently composed, best promotes efficiency and competition.

Separately, I've asked staff how we can bring greater transparency and resiliency to the ways in which U.S. Treasury securities are bought and sold across the market. Early in the pandemic, we witnessed a deterioration of liquidity affecting critical parts of the Treasury market. We also saw challenges in this market in September 2019 and in October 2014.

I've asked staff to work closely with our colleagues at the U.S. Department of the Treasury, the Federal Reserve, and the Commodity Futures Trading Commission to determine whether we can bring greater transparency and resiliency to these markets.

This work could build on Commission action last year to increase operational transparency to a subset of platforms as well as previous reforms regarding post-trade reporting. I've also asked staff to consider the potential benefits of central clearing in the Treasury cash and repo markets.

Whether it's equity markets, Treasury markets, or any other markets for that matter, for me it all comes down to how we best promote efficiency and maintain resilient markets in light of new business models and technologies.

Transparency

Finally, I will briefly discuss how we might consider updating various rules related to transparency.

One such area is beneficial ownership. In 1968, our Congress mandated that large shareholders of public companies disclose information that helps the public understand their ability to influence or control that company. Under current rules, beneficial owners of more than 5 percent of a public company's equity securities who have control intent have 10 days to report their ownership.

We haven't updated that deadline in over 50 years. Those rules might've been appropriate for the 1970s, but I have my doubts about whether they continue to make sense given the rapidity of current markets and technologies. I've asked staff how we might update these rules, including possibly shortening reporting deadlines.

Another area is around security-based swaps — essentially, derivatives on individual companies that provide exposure to the company without traditional equity ownership. The disclosures there aren't as robust as they are in the rest of the market. The collapse in March of the family office Archegos Capital Management is a reminder of why that could be relevant.

Thirdly, I think we can bring more transparency to short selling. We have unused authorities in that space that were granted by Congress nearly a dozen years ago.

Finally, I've asked staff to consider whether we should enhance transparency related to companies buying back their stock.

When investors cannot access critical information, particularly when some other market participants may have such information, such information asymmetry can increase risk and reduce liquidity. I believe we should update the transparency regimes to better reflect current business models and practices.

Before I close, I said I'd come back to LIBOR. In my last speech here, I said it was critical for regulators to "identify alternative interest rate benchmarks" with a robust underlying market. Eight years and a different job later, I still feel that way.

To that end, I have concerns that as LIBOR is replaced, a number of commercial banks are advocating for replacement indices that are still reliant on short-term, unsecured, bank-to-bank lending.

One such rate, called the Bloomberg Short-Term Bank Yield Index (BSBY), has many of the same flaws as LIBOR. They both rely on a relatively thin market that tends to disappear in times of stress.

Like with LIBOR, we're seeing a modest market, shouldering the weight of hundreds of trillions of dollars in transactions. When a benchmark is mismatched like that, there's a heck of an economic incentive to manipulate it.

When I last spoke here, I basically said the emperor had no clothes. At the time, the emperor was LIBOR. But make no mistake: Though we might gussy it up, short-term, unsecured, bank-to-bank lending is still the same emperor with no clothes.

I'll leave you with that. Thank you.

Central Bank Digital Currency and the future: Visa publishes new research

Cuy Sheffield, Head of Crypto, Visa - Report explores the offline exchange of digital cash and how it could benefit consumers and economies

In the past few years, a growing number of central banks have begun exploring new financial technologies and how they might enhance the stability, resiliency and efficiency of financial systems.

Now more than ever, governments around the world are focused on mechanisms for jumpstarting growth and providing financial relief to people, businesses and communities. In this context, interest in Central Bank Digital Currency, or CBDC, has accelerated.

CBDC represents a new form of money issued by a country's central bank directly to its citizens. But unlike traditional paper currencies, such as the U.S. dollar or euro, CBDC would exist exclusively in digital form.

Many central banks see CBDC as a way to provide a "digital version of cash," meaning that you would be able to receive and spend it directly, for example via a digital wallet on your phone or tablet.

This would be particularly valuable in countries where the infrastructure for distributing cash is unavailable or limited, a factor that can hinder central banks' efforts to bring people into the formal financial system.

Nevertheless, while several countries have taken concrete steps to advance a CBDC framework, most central banks are still in the exploratory phase.

Unlocking the economic potential

For many, the appeal of central bank-backed "digital cash" may seem vague, given the array of digital tools available for managing all aspects of our financial lives.

We tap a card to buy groceries, receive our paychecks electronically and pay our bills online. So what benefits, then, could CBDC offer a consumer who is already spending and receiving dollars digitally?

It depends on the person, their payment and banking needs and the context in which they work, live and transact.
There is no 'one-size-fits-all' in payments and banking. Traditional currencies and the ecosystems built around them serve people and businesses, safely and efficiently, in economies around the globe.

However, there are particular contexts and use cases where CBDC might offer distinct advantages.

For example, thanks to the cash-like and digital nature of CBDC, governments would be able to rapidly transfer funds to targeted groups of individuals and businesses, when and where they're needed most and in parts of the world where traditional banking services are not universally used.

The motivations driving central banks to explore CBDC are varied, but one objective that many seem to share is expanding financial inclusion, or helping unbanked individuals gain access to useful financial products and services.

While central banks differ on how to broaden financial inclusion with CBDC, the technology has the potential to more easily and securely connect someone to a vibrant ecosystem of accessible Fintechs and other financial products.

Tackling design hurdles

As central banks consider frameworks for reaping the benefits of CBDC, some common design challenges have emerged. For example, how might digital currencies be exchanged in person, when neither the buyer nor the seller has a connection to the internet?

Today the only reliable, real-time medium of exchange in an offline context is physical cash. For CBDC to have utility as an alternative to physical cash, it must be useable for face-to-face transactions occurring offline.

Visa has published a technical paper that outlines a novel approach for offline point-to-point payments between two devices. The protocol allows digital money to be directly downloaded onto a personal device, such as a smartphone or tablet. You may visit: https://arxiv.org/abs/2012.08003

The money is stored on a secure hardware embedded in that device and managed by a wallet provider (e.g. a bank). CBDC can be transacted from one device to another device directly without any intermediaries such as banks, payment networks, or payment processors. Examples of the underlying technology that can support point-to-point payments include Bluetooth and Near Field Communication (NFC).

The offline payment system, put simply, creates an experience similar to physical cash. But instead of paper in your wallet, it's bits and bytes in your phone.

You can imagine this functionality being useful where internet connectivity is intermittent and a user may only gain full connectivity periodically, say by visiting a local internet café.

To read more: https://usa.visa.com/visa-everywhere/blog/bdp/2020/12/17/central-bank-digital-1608165518834.html

https://arxiv.org/abs/2012.08003

Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies

Mihai Christodorescu[*], Wanyun Catherine Gu[**], Ranjit Kumaresan[*], Mohsen Minaei[*], Mustafa Ozdayi[*], Benjamin Price[**], Srinivasan Raghuraman[*], Muhammad Saad[*], Cuy Sheffield[**], Minghua Xu[*], and Mahdi Zamani[*]

[*]*Visa Research, Palo Alto, CA*
[**]*Visa Crypto Product, Palo Alto, CA*

Investor Alerts and Bulletins

Funds Trading in Bitcoin Futures

U.S. SECURITIES AND EXCHANGE COMMISSION

The Securities and Exchange Commission's (SEC's) Office of Investor Education and Advocacy (OIEA) and the Commodity Futures Trading Commission's (CFTC's) Office of Customer Education and Outreach (OCEO) urge investors considering a fund with exposure to the Bitcoin futures market to weigh carefully the potential risks and benefits of the investment.

Among other things, investors should understand that Bitcoin, including gaining exposure through the Bitcoin futures market, is a highly speculative investment.

As such, investors should consider the volatility of Bitcoin and the Bitcoin futures market, as well as the lack of regulation and potential for fraud or manipulation in the underlying Bitcoin market.

Bitcoin. Bitcoin is a digital asset, or an asset that relies on blockchain technology. Bitcoin has also been called a "virtual currency" or a "cryptocurrency."

Bitcoin future. A Bitcoin futures contract is a standardized agreement to buy or sell a specific quantity of Bitcoin at a specified price on a particular date in the future. In the United States, Bitcoin is a commodity, and commodity futures trading is required to take place on futures exchanges regulated and supervised by the CFTC.

Funds regulated under the Investment Company Act of 1940 and its rules ("funds") are required to provide important investor protections.

For example, funds must comply with legal requirements related to valuation and custody of fund assets, and mutual funds and ETFs must comply with liquidity requirements.

Those protections apply to all of a fund's holdings, including holdings of Bitcoin futures contracts.
Some funds may engage in the trading of Bitcoin futures contracts as one way to gain exposure to Bitcoin. Investors should understand that positions in Bitcoin and Bitcoin futures contracts are highly speculative.

Investors who are thinking about investing in a fund that buys or sells Bitcoin futures should carefully consider:

- *The investor's risk tolerance*. Investors should focus on the level of risk they are taking compared to the level of risk they are comfortable taking. For more information, read Assessing Your Risk Tolerance.

- *The fund's disclosure of its risks*. A fund is required to disclose the principal risks of investing in the fund in its prospectus. For more information read, How to Read a Mutual Fund Prospectus (Part 1 of 3: Investment Objective, Strategies, and Risks).

- *Potential loss of the investment*. All investments in funds involve risk of financial loss. This risk may be increased for positions in Bitcoin futures contracts because of the high volatility of Bitcoin and Bitcoin futures (meaning prices can fluctuate widely). There is also the potential for fraud and manipulation in the underlying cash or "spot" Bitcoin market.

- *Difference in investment outcome*. A rise in Bitcoin prices may not result in a similar increase in the value of a fund holding positions in Bitcoin futures contracts.

  This is in part because funds that trade commodity futures contracts may not have direct exposure to the contracts' underlying assets.

  Futures contract prices can vary by delivery months and differ from the underlying commodity's spot price.

  Futures contracts also expire periodically, resulting in fluctuations of portfolio exposure as expiring futures positions are typically rolled into new contracts.

  The value of a particular fund may be affected by this maintenance of futures contract exposure.

  For more information about funds or exchange traded products that trade commodity futures, see Learn About Risks Before Investing in Commodity ETPs or Funds. You may visit: https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CustomerAdvisory_CommodityETPs.htm

Funds that buy or sell Bitcoin futures may have unique characteristics and heightened risks compared to other funds. It is important to consider how any investment fits into your overall investment plan before investing.

Note: This Investor Bulletin represents the views of the staff of the SEC's Office of Investor Education and Advocacy and CFTC's Office of Customer Education and Outreach. It is not a rule, regulation, or statement of the Securities and Exchange Commission or the Commodity Futures Trading Commission (the "Commissions").

The Commissions have neither approved nor disapproved its content. This Bulletin, like all staff statements, has no legal force or effect: it does not alter or amend applicable law, and it does not create any enforceable rights or new or additional obligations for any person.

Joint ECB/ESRB report shows uneven impacts of climate change for the EU financial sector

- Financial stability vulnerabilities from climate change concentrated in certain regions, sectors and firms, with evolution of risks conditional on effective and timely transition to low carbon economy

- Granular exposure mapping of climate hazards to financial risk reveals vulnerability to river flooding widespread across countries, compounded by wildfire, heat and water stress risk in some regions

- Transition risk resulting from financial market repricing has cross-sector impact and varies within sectors owing to differences in emissions efficiency

- Long-term scenario analyses suggest timely and orderly macroeconomic policies to tackle climate-related risk can reduce financial stability risks, notably for highest greenhouse-gas emitting sectors

The European Central Bank (ECB) and the European Systemic Risk Board (ESRB) published a joint report that takes a closer look at how a broadened set of climate change drivers affects millions of global firms and thousands of financial firms in the European Union (EU). It maps out prospective financial stability risks and contributes by further developing the analytical basis for more targeted and effective policy action. The report: https://www.ecb.europa.eu/pub/pdf/other/ecb.climateriskfinancialstability202107~87822fae81.en.pdf

The report tackles measurement gaps and, building on previous work in this field, establishes a detailed topology of physical and transition risks

arising from climate change across regions, sectors and firms. It also applies a scenario analysis with long-dated financial risk horizons to capture prospective financial losses resulting from the timeliness and effectiveness of climate policies and technologies.

“These findings underline the crucial and urgent need for climate policies and economic transitions, not only to ensure that the targets of the Paris Agreement are met, but also to limit the long-run disruption to our economies, businesses and livelihoods,” said Christine Lagarde, President of the ECB and ESRB Chair.

The report’s granular mapping of financial exposures to climate change drivers finds three forms of risk concentration.

First, exposures to physical climate hazards are concentrated at the regional level. The analysis shows, for example, that river floods will be the most economically significant widespread climate risk driver in the EU over the next two decades compounded by strong vulnerability to wildfires, heat and water stress in some regions.

Around 30% of the euro area banking sector’s credit exposures to non-financial companies are to firms that are subject to a combination of these physical hazards.

Second, exposures to emission-intensive firms are concentrated not only across but also within economic sectors.

Exposures to highly emitting firms occupy 14% of collective euro area banking sector balance sheets. While mainly concentrated in the manufacturing, electricity, transportation and construction sectors, they also vary considerably within sectors – suggesting scope for financial market repricing as widely varying emissions intensities narrow.

Third, exposures to climate risk drivers are concentrated in specific European financial intermediaries.

Around 70% of banking system credit exposures to firms subject to high or increasing physical risk over the coming decades are concentrated in the portfolios of just 25 banks.

At the same time, scope for financial market repricing associated with transition risk will be particularly large for investment funds, where more than 55% of investments are tilted toward high emitting firms and estimated alignment with the EU Taxonomy stands at only 1% of assets. While direct holdings by insurers of climate sensitive assets may be

manageable, risks could be amplified by cross-holdings of investment funds of around 30%.

Long-term scenario analysis for EU banks, insurers and investment funds suggests that credit and market risk could increase as a result of a failure to effectively counteract global warming.

In the projected scenario modelling what would happen in the event of an insufficiently orderly climate transition, physical risk losses – particularly for high emitting firms – would become dominant in around 15 years. This could lead to a decline in global GDP of up to 20% by the end of the century should mitigation prove to be insufficient or ineffective.

As work continues on more accurately measuring and modelling climate risk, the advances described in this report should provide valuable evidence to inform the broadening climate debate in the public and private sector alike.

Climate stress testing – a new kid on the block

Climate-related risk and financial stability - ECB/ESRB Project Team on climate risk monitoring

In recent years progress has been made on climate stress testing and scenario analysis methodologies. This has been possible thanks to growing experience and the increased availability of datasets.

The following three sections discuss the challenges of climate-related scenario analysis for the financial sector.

The first two discuss trends in the area of forward-looking scenario analysis, while the third and the last section of the report puts these methodologies into use in a coordinated climate-sensitivity analysis of the European financial sector.

The Handbook in Annex 2 “Detailed look at existing methodologies” provides a complete overview of off-the-shelf methodologies developed in European institutions.

The Handbook is designed as a practical guide for practitioners and aims to foster the development of climate-related methodologies in other institutions.

It describes in detail different approaches to estimate key parameters that connect the non-financial sector, which could be impacted by climate-related shocks, and the financial sector’s balance sheets.

Since the publication of the first report of the ECB/ESRB Project Team on climate risk monitoring, central banks and supervisors have intensified their efforts to develop climate-related stress testing frameworks.

International organisations have also joined the call to incorporate climate-related risks in stress-testing exercises, including the International Monetary Fund (IMF) (2020a, 2020b), the Bank for International Settlements (BIS) (2020), the Financial Stability Board (FSB) (2020, 2021), and the Network for Greening the Financial System (NGFS) (2021).

European Union authorities have completed or are in the process of conducting or planning 18 climate stress test exercises.
The climate-related scenario analysis is gradually shifting towards stressing both physical and transition risks. As shown in Chart 16 (left panel), all of the stress testing and sensitivity initiatives completed up to

2020 focus on transition risks. However, from 2021 there is a growing number of exercises covering physical and transition risks.

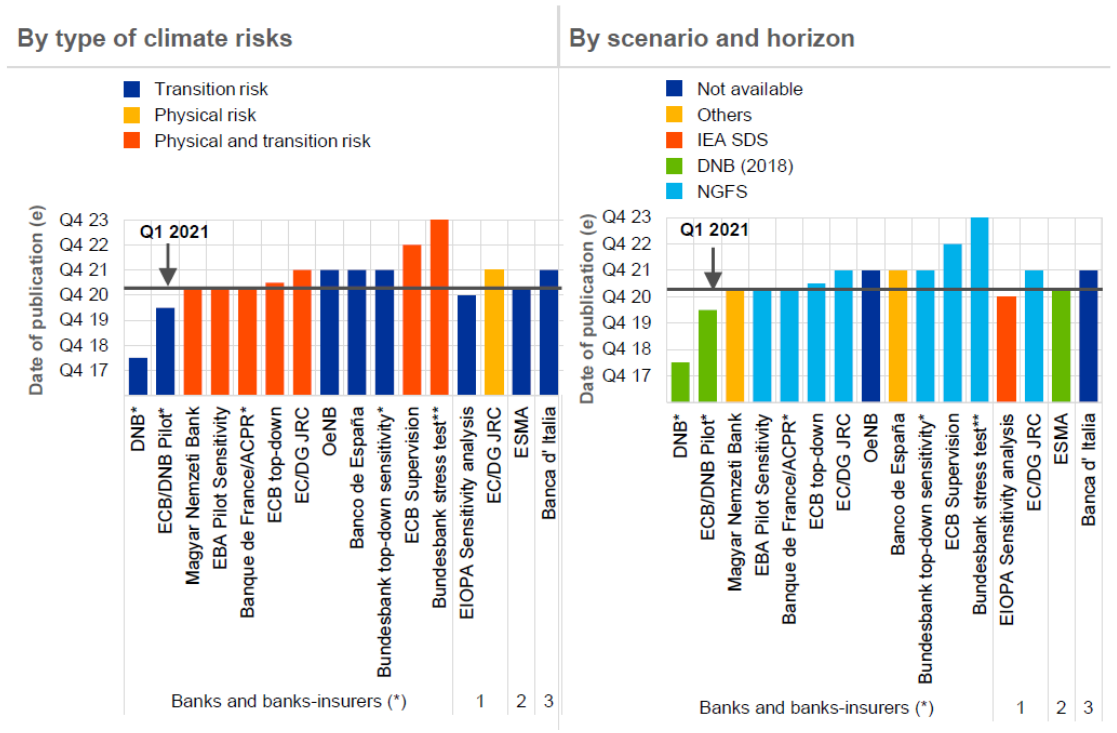
This trend is coupled with an extension of the horizon used in scenario analysis (Chart 16, right panel). The initial transition risk-focused stress test exercises relied on scenarios with a five-year horizon.

This was an extension compared with the more standard three-year horizon used in regular stress test exercises, but far shorter than the horizon of up to the year 2100 included in NGFS scenarios.

The ongoing exercises are bolder, extending to a 30-year horizon in most cases. The NGFS scenarios are becoming a common reference for ongoing and planned exercises, in particular, the orderly transition, the disorderly transition (with two variants, namely with effective and ineffective transition policies) and the "hot house world" scenario discussed in Section 6.

Chart 16

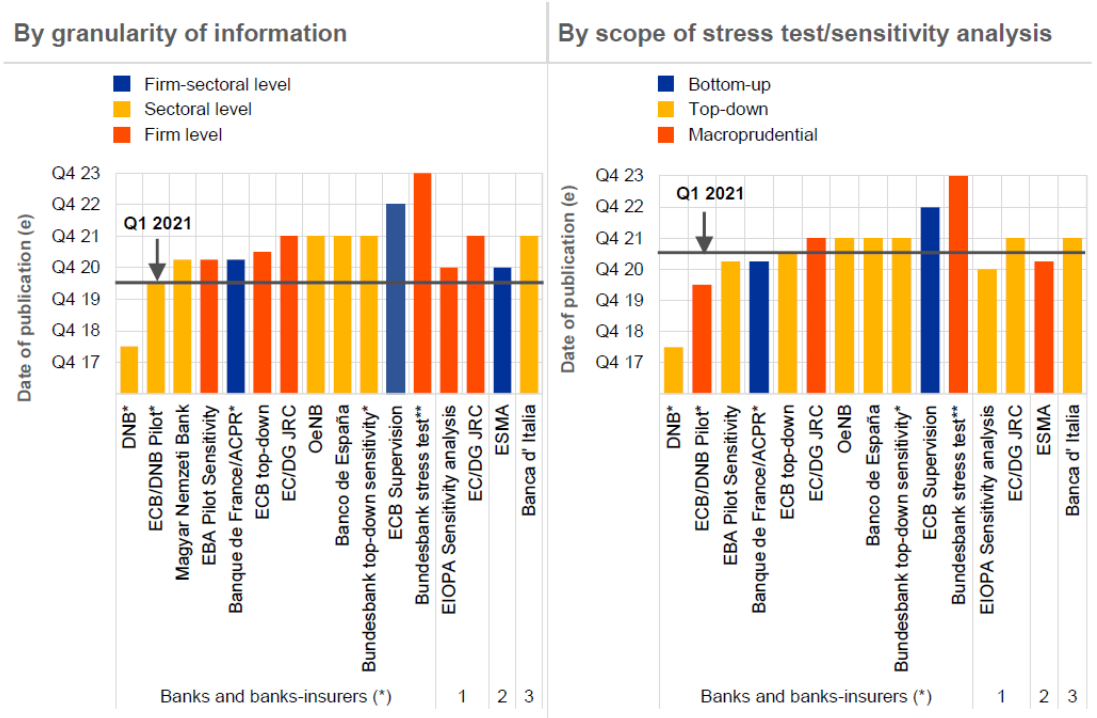
Initiatives of climate-related stress test and sensitivity analysis in European Union institutions



Climate-related stress-testing and sensitivity frameworks have evolved towards the use of increasingly granular data. As shown in Chart 17 (left panel), early exercises employed mostly sector-level information, e.g. sector-level CO_2 intensity.

Chart 17

Initiatives of climate-related stress test and sensitivity analysis in European Union institutions



It reflected the fact that disclosure of climate-related risks from private entities has been insufficient, heterogeneous and patchy.

As databases of climate risk and exposure information have been gradually improving and are made available, several institutions have started or are planning stress-testing exercises extensively using firm-level information or, in some cases, transaction-level information.

To read more (at page 51/111) you may visit:
https://www.ecb.europa.eu/pub/pdf/other/ecb.climateriskfinancialstability202107~87822fae81.en.pdf

Phishing most common Cyber Incident faced by SMEs

The European Union Agency for Cybersecurity identifies the cybersecurity challenges SMEs face today and issues recommendations.

Small and medium-sized enterprises (SMEs) are considered to be the backbone of Europe's economy. 25 millions of SMEs are active today in the European Union and employ more than 100 million workers.

The report Cybersecurity for SMEs ENISA issues today provides advice for SMEs to successfully cope with cybersecurity challenges, particularly those resulting from the COVID-19 pandemic.

With the current crisis, traditional businesses had to resort to technologies such as QR codes or contactless payments they had never used before.

Although SMEs have turned to such new technologies to maintain their business, they often failed to increase their security in relation to these new systems.
Research and real-life experience show that well prepared organisations deal with cyber incidents in a much more efficient way than those failing to plan or lacking the capabilities they need to address cyber threats correctly.
Juhan Lepassaar, EU Agency for Cybersecurity Executive Director said:
“SMEs cybersecurity and support is at the forefront of the EU’s cybersecurity strategy for the digital decade and the Agency is fully

dedicated to support the SME community in improving their resilience to successfully transform digitally."

In addition to the report, ENISA also publishes today the Cybersecurity Guide for SMEs: "12 steps to securing your business". The short cybersecurity guide provides SMEs with practical high-level actions to better secure their systems, hence their businesses.

Based on an extended desktop research, an extensive survey and targeted interviews, the report identifies those pre-existing cybersecurity challenges worsened by the impact of the pandemic crisis.

Key findings

85% of the SMEs surveyed agree that cybersecurity issues would have a serious detrimental impact on their businesses with 57% saying they would most likely go out of business.

Out of almost 250 SMEs surveyed, 36% reported that they had experienced an incident in the last 5 years. Nonetheless, cyberattacks are still not considered as a major risk for a large number of SMEs and a belief remains that cyber incidents are only targeting larger organisations.

However, the study reveals that phishing attacks are among the most common cyber incidents SMEs are likely to be exposed to, in addition to ransomware attacks, stolen laptops, and Chief Executive Officer (CEO) frauds.

For instance, with the concerns induced by the pandemic, cyber criminals seek to compromise accounts using phishing emails with Covid-19 as a subject.

CEO frauds are other decoys meant to lure an employee into acting upon the instructions of a fraudulent email displayed as if sent from their CEO, and usually requesting a payment to be performed in urgency under business-like circumstances.

The report unveils the following challenges SMEs are faced with:

- Low awareness of cyber threats;
- Inadequate protection for critical and sensitive information;
- Lack of budget to cover costs incurred for implementing cybersecurity measures;
- Availability of ICT cybersecurity expertise and personnel;
- Absence of suitable guidelines tailored to the SMEs sector;
- Moving online;

- Low management support.

How to address those challenges?

The recommendations issued fall into three categories:

People

People play an essential role in the cybersecurity ecosystem. The report draws attention to the importance of responsibility, employee buy-in and awareness, cybersecurity training and cybersecurity policies as well as third party management in relation to confidential and/or sensitive information.

Processes

Monitoring internal business processes include performing audits, incident planning and response, passwords, software patches and data protection.

Technical

At the technical level, a number of aspects should be considered in relation to network security, anti-virus, encryption, security monitoring, physical security and the securing of backups.

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.