International Association of Hedge Funds Professionals (IAHFP)
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.hedge-funds-association.com

Hedge Funds News, September 2021

Dear members and friends,

We will start with the new *Joint Committee Report of the European Supervisory Authorities on Risks and Vulnerabilities in the EU Financial System*.

After over a year since the COVID-19 pandemic started, the financial sector has largely proved resilient in the face of its severe economic impact.

A range of fiscal, monetary and prudential response measures as well as the availability of capital buffers have been essential in dampening the impact of the crisis.

As the recovery begins, the appropriate phasing out of exceptional crisis measures plays a key role.

Despite the positive outlook, the expectations for economic recovery remain uncertain and uneven across member states. Vulnerabilities in the financial sector are increasing, not least because of side effects of the crisis

measures, such as increasing debt levels and upward pressure on asset prices.

Also, expectations of inflation- and yield growth, as well as increased investor risk-taking and financial interconnectedness issues, might put additional pressure on the financial system.

Next to economic vulnerabilities, the financial sector is also increasingly exposed to cyber risk and informationand communication technology (ICT) related vulnerabilities.

Financial institutions have to rapidly adapt their technical infrastructure in response to the pandemic, and the crisis has acted as a catalyst for digital transformation more generally.

The reliance of the financial system on technology and the scope for cyber vulnerabilities have further increased.

The financial sector has been hit by cyber-attacks more often than other sectors, while across the digital economy cyber-criminals are developing new techniques to exploit vulnerabilities.

In light of the above-mentioned risks and uncertainties, the Joint Committee advises the ESAs, national competent authorities, financial institutions and market participants to take the following policy actions:

1. Financial institutions and supervisors should continue to be prepared for a possible deterioration of asset quality in the financial sector, notwithstanding the improved economic outlook.

In light of persisting risks and high uncertainties, supervisors should continue to closely monitor asset quality and provisioning in the banking sector, in particular of assets under support schemes. This includes identifying possible practices of under-provisioning.

Such monitoring is an important prerequisite when coordinating the unwinding of the various support measures.

2. As the economic environment gradually improves, the focus should in particular shift to allow a proper recognition of the consequences of the pandemic on banks' lending books, and that banks adequately manage the transition towards the recovery phase.

Banks may need to withstand possibly increasing credit risk losses, as a consequence of expiring payment moratoria and other public support measures, while maintaining adequate lending volumes.

Banks and borrowers experiencing financial difficulties should proactively work together to find appropriate solutions for their specific circumstances.

That should include not only financial restructuring, but also a timely recognition of credit losses. Other financial institutions, including investment funds, should monitor their investments in corporate bonds and into private lending.

3. Disorderly increases in yields and sudden reversals of risk premia should be closely monitored in terms of their impacts for financial institutions as well as for investors.

On the investor side, rising valuations across asset classes, massive price swings in crypto assets, and event-driven risks (such as GameStop, Archegos, Greensill) observed in 1Q21 amid elevated trading volumes raise questions about increased risk-taking behaviour and possible market exuberance.

Rising yields could result in higher funding costs for banks and increase default risks for corporates via higher borrowing costs.

Supervisors, policy makers and financial institutions should also continue to develop further actions to accommodate a "low-for-long" real interest rate environment and risks its entails against the background of rising in inflation. This includes addressing overcapacities in the financial sector.

4. Policymakers, regulators, financial institutions and supervisors can start reflecting on lessons learnt from the COVID-19 crisis. While the EU economy is still subject to high risks, some lessons learnt have, for example, already been reflected in EIOPA's advice on the Solvency II review.

EIOPA recommends in its opinion that supervisors should have additional powers, including a macroprudential toolkit to tackle systemic risk, such as restrictions on distributions of dividends to preserve insurers' financial position in periods of extremely adverse developments.

In the banking sector, the crisis has underlined the need to advance the Banking Union, and to achieve its potential additional benefits of cross-border financial flows, private risk sharing, and exploiting economies of scale in a larger market.

The ongoing crisis also highlighted the critical importance of coordinated approaches among national competent authorities.

5. Financial institutions and supervisors should continue to carefully manage their ICT and cyber risks. They should ensure that appropriate technologies and adequate control frameworks are in place to address threats to information security and business continuity, including risks stemming from increasingly sophisticated cyber-attacks.

It will be important for EU financial institutions to achieve a high common level of digital operational resilience, and to swiftly put in place an EU-wide common framework for digital operational resilience.

An important aspect of digital operational resilience is proper management of risks around ICT outsourcing, including chain outsourcing. Additionally, there is increasingly a need for financial institutions to carry out resilience testing in proportion to the risks faced and in a consistent manner.

To read more: https://www.eiopa.europa.eu/sites/default/files/joint-committee/jc-2021-45-joint-committee-autumn-2021-report-on-risks-and-vulnerabilities.pdf?fbclid=IwAR1kJP7I_WF41wzeot_GQAb1P2NbcLB1AnucPdb2eNeuV4167HJVzRBlRZk

JOINT COMMITTEE REPORT ON

RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM

SEPTEMBER 2021

Executive summary and Policy actions **2**
Introduction **3**
1 Market developments **4**
2 Developments in the financial sector **5**
3 Transition/exit from COVID-19 crisis and ongoing risks **6**
3.1 Vulnerabilities in the financial sector 6
3.2 Financial sector exposure to the public and corporate sectors 9
3.3 Potential risks from rapidly increasing yields in the low interest rate environment 10
4 ICT and cyber risks – recent developments and reinforcement due to the covid-19 crisis **11**

ESMA Report on Trends, Risks and Vulnerabilities

esma European Securities and Markets Authority

Risk summary

EU financial markets continued their recovery during the first half of 2021 with valuations at or above pre-COVID-19 levels, as the global economic outlook improved, with COVID-19 vaccine roll-outs and amid sustained public policy support.

Fixed income valuations, notably for HY corporate bonds are now far above their pre-COVID-19 levels in a context of increasing corporate and public debt.

Increased risktaking behaviour has led to volatility in equity (e.g. GameStop related market movements) and crypto asset markets, as well as to the materialisation of event-driven risks such as in the case of Archegos or Greensill.

Going forward, we expect to continue to see a prolonged period of risk to institutional and retail investors of further – possibly significant – market corrections and see very high risks across the whole of the ESMA remit.

Current market trends will need to show their resilience over an extended period of time for a more positive risk assessment to be made.

The extent to which these risks will materialise will critically depend on market expectations on monetary and fiscal policy support, as well as on the pace of the economic recovery and on inflation expectations.

ESMA remit	Level	Outlook
Overall ESMA remit	■	→
Securities markets	■	→
Infrastructures and services	■	→
Asset management	■	→
Consumers	■	↗

Risk categories	Level	Outlook
Liquidity	■	→
Market	■	→
Contagion	■	↗
Credit	■	↗
Operational	■	→

Risk drivers	Outlook
Macroeconomic environment	↘
Interest-rate environment	→
Sovereign and private debt markets	↗
Infrastructure disruptions	→
Political and event risks	↗

Note: Assessment of the main risks by risk segments for markets under ESMA's remit since the last assessment, and outlook for the forthcoming quarter. Assessment of the main risks by risk categories and sources for markets under ESMA's remit since the last assessment, and outlook for the forthcoming quarter. Risk assessment is based on the categorisation of the European Supervisory Authorities (ESA) Joint Committee. Colours indicate current risk intensity. Coding: green=potential risk, yellow=elevated risk, orange=high risk, red=very high risk. Upward-pointing arrows indicate an increase in risk intensity, downward-pointing arrows a decrease and horizontal arrows no change. Change is measured with respect to the previous quarter; the outlook refers to the forthcoming quarter. ESMA risk assessment based on quantitative indicators and analysts' judgement.

Table of contents 3

Executive summary 4

Market monitoring 7
Market environment 8
Market trends and risks 10
Securities markets 10
Infrastructures and services 15
Asset management 22
Consumers 31
Market-based finance 36
Sustainable finance 44
Financial innovation 52

Risk analysis 62
Financial stability 63
Cloud outsourcing and financial stability risks 63
Financial stability 72
COVID-19 and credit ratings 72
Investor protection 82
The market for small credit rating agencies in the EU 82
Investor protection 95
Environmental impact and liquidity of green bonds 95
TRV statistical annex 107
List of abbreviations 108

The report:
https://www.esma.europa.eu/sites/default/files/library/esma50-165-1842_trv2-2021.pdf

Central bank digital currency: the future starts today

Benoît Cœuré, Head of the BIS Innovation Hub, at The Eurofi Financial Forum, Ljubljana

Distinguished guests, ladies and gentlemen.

Thank you for inviting me to speak here today. We all experienced how the pandemic accelerated the shift to virtual events, but I am pleased that today we are gathering in person.

Yet the world is not returning to the old normal. Payments are a case in point. The pandemic has accelerated a longer-running move to digital.

Mobile and contactless payments are already part of our daily lives; QR codes and "buy now, pay later" options are gaining popularity; gloves, badges and Olympic uniforms with payment functions are being prepared for the Beijing Winter Olympics; and the tech-savvy generation will soon dream about money and payments for the metaverse.

Alongside these developments, the world's central banks are stepping up efforts to prepare the ground for digital cash – central bank digital currency (CBDC). They have a job to do – delivering price stability and financial stability – and they must retain their ability to do it.

Let me explain.

Central bank money has unique advantages – safety, finality, liquidity and integrity. As our economies go digital, they must continue to benefit from these advantages.

Money is at the heart of the system and it has to continue to be issued and controlled by trusted and accountable institutions which have public policy – not profit – objectives.

Central bank money will have to evolve to be fit for the digital future.

So what are the priorities now? Know where you are going – as Dag Hammarskjöld once said2, "only he who keeps his eye fixed on the far horizon will find the right road". And get going.

Let me elaborate.

Why do we need to know where are we going? Because today, the financial system is shifting under our feet.

Big techs are expanding their footprint in retail payments. Stablecoins are knocking on the door, seeking regulatory approval. Decentralised finance (DeFi) platforms are challenging traditional financial intermediation. They all come with different regulatory questions, which need fast and consistent answers.

Banks are worried about the implications of CBDCs for customer deposits. Central banks are mindful of these concerns and are working on answers. They see banks as part of future CBDC systems. But make no mistake: global stablecoins, DeFi platforms and big tech firms will challenge banks' models regardless.

Stablecoins may develop as closed ecosystems or "walled gardens", creating fragmentation. With DeFi protocols, any concerns about the assets underlying stablecoins could see contagion spread through a system. And the growing footprint of big techs in finance raises market power and privacy issues, and challenges current regulatory approaches.

Will the new players complement or crowd out commercial banks? Should central banks open accounts to these new players, and under which regulatory conditions? Which kind of financial intermediation do we need to fund investment and the green transformation? How should public and private money coexist in new ecosystems – for example, should central bank money be used in DeFi rather than private stablecoins?

We urgently need to ask ourselves these kinds of questions about the future. This is the far horizon for the financial system but we are approaching it ever faster. Central banks need to know where they want to go as they embark on their CBDC journey.

CBDC will be part of the answer. A well-designed CBDC will be a safe and neutral means of payment and settlement asset, serving as a common interoperable platform around which the new payment ecosystem can organise. It will enable an open finance architecture that is integrated while welcoming competition and innovation. And it will preserve democratic control of the currency.

This brings me to my second message: the time has passed for central banks to get going. We should roll up our sleeves and accelerate our work on the nitty-gritty of CBDC design. CBDCs will take years to be rolled out,

while stablecoins and cryptoassets are already here. This makes it even more urgent to start.

In the design thinking methodologies we use in the BIS Innovation Hub, the ideal product stands in a sweet spot at the intersection of desirability, viability and feasibility. When applied to CBDCs, these translate into three dimensions: consumer use cases, public policy objectives and technology.

We have to ask ourselves why consumers would want a CBDC and what would they want it to do? The recent European Central Bank (ECB) public consultation showed that they value privacy, security and broad usability.

In order to meet consumers' expectations, CBDCs need to be made to work most conveniently. Payment data must be protected. Digital functions that are not available with cash can be developed, such as programmability or viable micro-payments.

Then CBDCs should meet public policy objectives. Central banks exist to safeguard monetary and financial stability for the public good. CBDCs are a tool to pursue this through enhancing safety and neutrality in digital payments, financial inclusion and access, innovation and openness. Important questions remain. How can CBDC systems interoperate, and should offshore use be discouraged?

Technology opens up design choices. System design will be complex. It involves a hands-on operational and oversight role for central banks and public-private partnerships to develop the core features of the CBDC instrument and its underlying system. These features are: ease of use, low cost, convertibility, instant settlement, continuous availability and a high degree of security, resilience, flexibility and safety.

Complex trade-offs will be addressed by central banks including how to balance scale, speed and open access with security; and how to balance offline functionality with complexity and security.

Across the world, central banks are coming together to focus on their common mission. Charged with stability, they will not rush. They want to move fast, but not to break things.

Consultations with payment systems and providers, banks, the public and a broad range of stakeholders have begun in some countries. To build a CBDC for the public, a central bank needs to understand what they need, and work closely with other authorities. The BIS Innovation Hub is helping central banks. We already have six CBDC-related proofs of concept and prototypes being developed in our centres, and more to come.

The European Union is uniquely placed to face the future. You can build on a state-of-the-art fast payment system, on the strong protections provided by the General Data Protection Regulation and on the open philosophy of the Second Payment Services Directive. The ECB's report on a digital euro sets the stage.

A CBDC's goal is ultimately to preserve the best elements of our current systems while still allowing a safe space for tomorrow's innovation. To do so, central banks have to act while the current system is still in place – and to act now.

I thank you for your attention.

Basel III implementation in the European Union

Introductory remarks by Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, Eurofi panel on Basel III implementation in the EU, Ljubljana

Good morning and welcome to this panel on implementing Basel III in the EU.

When I was asked to chair this panel (in my capacity as Chair of the Basel Committee), I must confess that I had somewhat mixed feelings.

On the one hand, I was pleased to see that Eurofi was organising this one-hour panel to discuss what is a crucially important topic. As you know, following the Great Financial Crisis (GFC), the Basel Committee undertook a range of reforms to address material regulatory fault lines in the banking system.

The benefits of the initial set of reforms – which were aimed at addressing the unsustainable levels of leverage in the banking system, insufficient high-quality capital, excessive maturity transformation and lack of a macroprudential overlay – were clear to all of us during this pandemic.

The global banking system has remained broadly resilient to date, and, unlike during the GFC, banks have not exacerbated the economic crisis by sharply cutting back lending. The initial Basel III reforms, alongside an unprecedented range of public support measures, are the main explanations for this outcome.

In many ways, Covid-19 has provided clear and tangible evidence of the benefits to society in having a well-capitalised banking system. We saw that jurisdictions with banks that had the largest capital buffers experienced a less severe impact on their expected GDP growth and better-capitalised banks increased their lending more during the pandemic relative to their peers.

Yet the job of safeguarding global financial stability is far from finished. The outstanding Basel III reforms, which were finalised in 2017, are aimed at addressing significant fault lines in the global banking system. Addressing these fault lines remains as important today as it was pre-pandemic. Indeed, the primary objective of these reforms is to restore credibility in the risk-weighted capital framework. This is to be achieved by

reducing excessive variability in banks' modelled capital requirements and developing robust risk-sensitive standardised approaches which would also serve as the basis of the output floor.

Recall how at the peak of the GFC investors lost faith in banks' published ratios and placed more weight on other indicators of bank solvency. Whether due to a lack of robustness in banks' models or an excessive degree of discretion in determining key regulatory inputs, the shortcomings in the risk-weighted asset (RWA) framework underlined the need for a complete overhaul.

Let me just give one example to underline how these fault lines continue to remain a major concern today. In 2013, the Committee's first report on the variability of banks' risk-weighted assets highlighted a worrying degree of variation.

When banks were asked to model their credit risk capital requirements for the same hypothetical portfolio, the reported capital ratios varied by 400 basis points.

Fast-forward to 2021 – eight years later – and despite repeated claims by some stakeholders that banks have already "fixed" this problem, the latest report by the European Banking Authority on banks' modelled capital requirements points to a "significant" level of capital dispersion "that needs to be monitored".

Importantly, these Basel III reforms are not an exercise to increase overall capital requirements at a global level. But equally, to successfully meet our primary objective, "outlier" banks, such as those with particularly aggressive modelling techniques, will rightly face higher requirements.

Given the "exogenous" nature of the Covid-19 shock, these vulnerabilities were not tested during this pandemic.

However, it is clear that, if left unaddressed, they will expose material shortcomings in the banking system in future financial crises. So I am pleased that we will have the opportunity this morning to discuss the implementation of these reforms in the EU.

On the other hand, I remain concerned about the potential to focus the discussion on whether or how to implement Basel III in the EU in the current juncture! These reforms were finalised in 2017, with a globally agreed (revised) implementation date of 1 January 2023. G20 Leaders have repeatedly called for their full, timely and consistent implementation. Now is therefore the time for action.

It is increasingly clear that the outstanding Basel III reforms will complement the previous ones in having a positive net impact on the economy.

For example, a recent analysis by the ECB suggests that the GDP costs of implementing these reforms in Europe are modest and temporary, whereas their benefits will help to permanently strengthen the resilience of the economy to adverse shocks.

It also finds that potential deviations from the globally agreed Basel III reforms – for example, with regard to the output floor – would significantly dilute the benefits to the real economy.

Importantly, the reforms also benefited from an extensive consultation process with a wide range of stakeholders. Indeed, a recent academic study described the Committee's consultation approach as "one of the most procedurally sophisticated" processes among policymaking bodies.

The Committee published no fewer than 10 consultation papers as part of these reforms, with an accompanying consultation period that spanned the equivalent of almost three years!

So the finalised standards agreed at the global level are already a compromise by their very nature, and reflect the different views of Committee members and external stakeholders. Over 35 key adjustments were made to the reforms during this period, with the majority of these reflecting the views of different European stakeholders.

Financial stability is a global public good. It knows no geographic boundaries – the adage that "no one is safe until everyone is safe" applies as much to the pandemic as it does to safeguarding global financial stability.

This is why the Committee designed and calibrated Basel III at a global level, and incorporated enough flexibility through national discretions within the framework.

Approaching these reforms from a different perspective – for example by giving undue attention to the impact on individual banks, jurisdictions or regions – risks missing the forest for the trees.

To be clear: the domestic and democratic transposition of global standards is a very important process and one that should be fully respected. But the focus should now primarily be on the "action" side of things, which means demonstrating how the EU's commitment to multilateralism and to globally agreed decisions endorsed by the Group of Governors and Heads

of Supervision, and to which G20 Leaders have repeatedly committed to implementing in a full, timely and consistent manner.

So I hope that our panel discussion today and the active participation of the audience will provide a constructive discussion on these important issues, building on the broad landscape that I have just set out.

ENISA threat landscape for supply chain attacks

Supply chain attacks have been a security concern for many years, but the community seems to have been facing a greater number of more organized attacks since early 2020.

It may be that, due to the more robust security protection that organizations have put in place, attackers successfully shifted towards suppliers.

They managed to have significant impacts in terms of the downtime of systems, monetary losses and reputational damages, to name but a few.

The importance of supply chains is attributed to the fact that successful attacks may impact a large amount number of customers who make use of the affected supplier.

Therefore, the cascading effects from a single attack may have a widely propagated impact.

This report aims at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021.

Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations.

It is estimated that there will be four times more supply chain attacks in 2021 than in 2020.

With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common nontargeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

This report presents the Agency's Threat Landscape concerning supply chain attacks, produced with the support of the Ad-Hoc Working Group on Cyber Threat Landscapes.

Table 1: Proposed taxonomy for supply chain attacks. It has four parts: (i) attack techniques used on the supplier, (ii) assets attacked in the supplier, (iii) attack techniques used on the customer, (iii) assets attacked in the customer.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software	Trusted Relationship [T1199]	Data
Social Engineering	Software Libraries	Drive-by Compromise [T1189]	Personal Data
Brute-Force Attack	Code	Phishing [T1566]	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
Exploiting Configuration Vulnerability	Data	Physical Attack or Modification	Processes
Open-Source Intelligence (OSINT)	Processes	Counterfeiting	Bandwidth
	Hardware		Financial
	People		People
	Supplier		

The main highlights of the report include the following:

- A taxonomy to classify supply chain attacks in order to better analyse them in a systematic manner and understand the way they manifest is described.
- 24 supply chain attacks were reported from January 2020 to early July 2021, and have been studied in this report.
- Around 50% of the attacks were attributed to well-known APT groups by the security community.
- Around 42% of the analysed attacks have not yet been attributed to a particular group.
- Around 62% of the attacks on customers took advantage of their trust in their supplier.
- In 62% of the cases, malware was the attack technique employed.
- When considering targeted assets, in 66% of the incidents attackers focused on the suppliers' code in order to further compromise targeted customers.

- Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people.

- Not all attacks should be denoted as supply chain attacks, but due to their nature many of them are potential vectors for new supply chain attacks in the future.

- Organizations need to update their cybersecurity methodology with supply chain attacks in mind and to incorporate all their suppliers in their protection and security verification.

To read more: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Table 2: Attack techniques used to compromise the supplier in the chain. Each technique identifies how the attack happened, and not what was attacked. Several techniques may be used in the same attack.

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

BIS Bulletin No 45, Regulating big techs in finance

Agustín Carstens, Stijn Claessens, Fernando Restoy and Hyun Song Shin

Key takeaways

- Big tech firms entering financial services can scale up rapidly with user data from their existing business lines in e-commerce and social media, and by harnessing the inherent network effects in digital services.

- In addition to traditional policy concerns such as financial risks, consumer protection and operational resilience, the entry of big techs into financial services gives rise to new challenges surrounding the concentration of market power and data governance.

- The current framework for regulating financial services follows an activities-based approach where providers must hold licences for specific business lines. There is scope to address the new policy challenges by developing specific entity-based rules, as proposed in several key jurisdictions – notably the European Union, China and the United States.

The centrality of data in the digital economy has enabled the entry into financial services and rapid growth of big tech firms.

Big techs have existing businesses in e-commerce and social media, among others, from which they can expand into finance.

Their business model revolves around the direct interactions of users and the data generated as an essential by-product of these interactions.

The distinguishing feature of big techs is that they can overcome limits to scale by utilising user data from their existing businesses to scale up rapidly by harnessing the inherent network effects in digital services.

In turn, the greater user activity generates yet more data, reinforcing the advantages that come from network effects.

In this way, big techs can establish a substantial presence in financial services very quickly through the so-called "data-networkactivities" (DNA) loop.

This gives rise to concerns about the emergence of dominant firms with excessive concentration of market power and a possibly systemic footprint in the financial system.

The rapid growth of big tech firms in financial services presents various policy challenges.

Some are variations of familiar themes that lie squarely within the traditional scope of central banks and financial regulators, such as the mitigation of financial risks and the oversight of operational resilience and consumer protection.

Assessing big techs' resilience through a financial cycle will necessitate more systematic monitoring and understanding of big tech business models on the part of the authorities, for instance on whether learning algorithms may inject systematic biases to the detriment of financial stability.

As well as issues that arise from traditional financial stability concerns, there are new and unfamiliar challenges stemming from the potential for excessive concentration of market power, as well as broader issues concerning data governance.

These new challenges lie outside the traditional scope of the central bank's remit, but they can nevertheless impinge on the central bank's core mission of ensuring sound money as well as the integrity and smooth functioning of the payment system.

While some central banks' oversight authority includes the competitive functioning and efficiency of the payment system, their mandates do not normally encompass the broad range of competition and data privacy issues that arise in relation to the activities of big techs in financial services.

Nevertheless, since the central bank issues the unit of account in the economy, trust in the currency rests ultimately on the trust placed in the central bank itself.

Any impact on the integrity of the monetary system arising from the emergence of dominant platforms ought to be a key concern for the central bank.

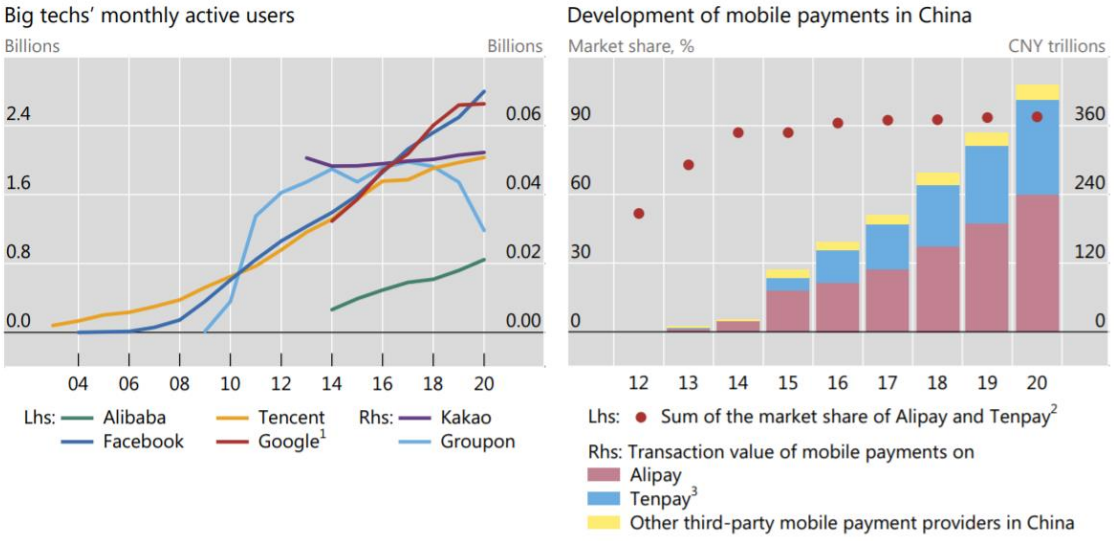
This Bulletin reviews the policy challenges for central banks and financial regulators in their oversight of the activity of big tech firms in financial services, especially as it relates to the payment system.

Traditional demarcations that separate the roles of financial regulators from those of competition authorities and data privacy regulators may become blurred in the case of big techs in finance.

Rules that were formulated with specific financial stability risks in mind (credit and liquidity risk, market risk etc) may be inadequate for addressing the unique combination of policy concerns to which big techs give rise.

These concerns bear on the central bank's core mission to maintain the integrity of the monetary system. In this regard, the central bank should work more closely with competition and data privacy authorities.

Big techs' rapid growth in users underpins their dominance in some markets — Graph 1



[1] The number of Chrome users is used as a proxy for Google's number of active users. [2] Market shares for 2012 are estimated based on market evidence. [3] Tenpay includes WeChat Pay and QQ Wallet.

Sources: BIS (2019); Enfodesk; S&P Capital IQ, company reports, analysys.cn; Statista, Industries; BIS calculations.

To read more: https://www.bis.org/publ/bisbull45.pdf

Risk Dashboard: European insurers' risk levels remain broadly stable

The European Insurance and Occupational Pensions Authority (EIOPA) published today its Risk Dashboard based on the first quarter of 2021 Solvency II data.

Risk Dashboard July 2021 (Q1-2021 Solvency II Data)

Risks	Level	Trend (past 3 months)	Outlook (next 12 months)
Macro risks	High	→	→
Credit risks	Medium	→	→
Market risks	Medium	→	→
Liquidity and funding risks	Medium	→	→
Profitability and solvency	Medium	↘	→
Interlinkages and imbalances	Medium	→	→
Insurance (underwriting) risks	Medium	→	→
Market perceptions	Medium	→	→

Note: The structural break as of Q1 2020 related to the Brexit withdrawal agreement and represented with a dashed line indicates a break in the number of undertakings of the time series and rebalance of the country weights. Additionally, adjusted time series for EU27 before Q1 2020 are also disclosed to reflect potential variations driven by the structural break in the sample.

The results show that insurers' exposures to macro risks remain at high level while all other risk categories remain at medium level.

With regards to macro risk, Gross Domestic Product growth and inflation forecasts registered new upward revisions. The 10 years swap rates have slightly increased across currencies in the second quarter of 2021.

Financial markets remain broadly stable, amid fiscal and monetary support.

Solvency positions for the first quarter of 2021 for all types of undertakings showed an improvement. Life insurers' profitability, measured by annual investments' returns, registered a notable deterioration in 2020.

Insurance risks remain at medium level, in spite of deterioration of some indicators.

The cumulative catastrophe loss ratio and year-on-year premium growth for non-life continued deteriorating.

On the other hand, the loss ratio decreased to one of the lowest values and year-on-year premium growth for life reported a slight recovery after the deterioration in the previous quarters.

Market perceptions remain at medium level with an increasing trend. The life insurance sector underperformed while non-life outperformed the stock market in the second quarter 2021.

Key observations

The results show that insurers' exposures to macro risks remain at high level while all other risk categories remain at medium level.

- With regards to macro risk, Gross Domestic Product growth and inflation forecasts registered new upward revisions. The 10 years swap rates have slightly increased across currencies in the second quarter of 2021.

- Financial markets remain broadly stable, amid fiscal and monetary support. Solvency positions for the first quarter of 2021 for all types of undertakings showed an improvement.

- Life insurers' profitability, measured by annual investments' returns, registered a notable deterioration in 2020.

- Insurance risks remain at medium level, in spite of deterioration of some indicators.

- The cumulative catastrophe loss ratio and year-on-year premium growth for non-life continued deteriorating.

- On the other hand, the loss ratio decreased to one of the lowest values and year-on-year premium growth for life reported a slight recovery after the deterioration in the previous quarters.

- Market perceptions remain at medium level with an increasing trend.

- The life insurance sector underperformed while non-life outperformed the stock market in the second quarter 2021.

To read more: https://www.eiopa.europa.eu/tools-and-data/risk-dashboard_en

Report on EIOPA Supervisory Activities in 2020

EIOPA's supervisory convergence plan for 2021 identifies one of the main goals of the European Insurance and Occupational Pensions Authority (EIOPA) by ensuring a high, effective and consistent level of supervision across Europe, with the aim of guaranteeing a similar level of protection of policyholders and beneficiaries across jurisdictions, preventing supervisory arbitrage and guaranteeing a level playing field.

As a step towards the implementation of the plan, this Report presents how EIOPA contributed during 2020 to enhancing the common European supervisory culture and promoted consistent supervisory practices both from a prudential and conduct of business supervision perspective.

The year of 2020 brought the world a pandemic which has created huge social disruptions and unprecedented economic challenges. EIOPA had adapted its priorities and strategies to support both industry and supervisors to tackle those different challenges.

To maintain supervisory convergence in a pandemic situation required cooperation and timely reaction.

The situation triggered some extraordinary and flexible responses.

In particular, EIOPA encouraged supervisors and insurers to make use of the flexibility embedded in the existing regulatory framework and issued some supervisory statements to deal with the new risks and situations caused by the pandemic.

The need to carry out activities previously not planned inevitably had the consequence to reprioritise some of the planned work.

Anyway, the work on supervisory convergence overall revealed a good degree of progress, covering a variety of areas, from Solvency II related issues such as calculation of technical provisions to further development of supervisory activities in the area of conduct risks and analysis of innovative technologies and how they can improve supervisory practices.

On conduct risks EIOPA finalised a chapter for the Supervisory Handbook containing guidance to supervisors on how to carry out a risk-based, outcome-focused and proportional supervision of Product Oversight and Governance (POG) requirements. EIOPA also published "EIOPA's approach to the supervision of product oversight and governance" aiming

at providing more clarity for insurance manufacturers and distributors on the supervisory approach to POG requirements.

Following up the request of the European Commission to EIOPA for a technical advice on the review of the Solvency II Directive in February 2019, EIOPA finalised its Advice in December 2020 leveraging on a number of activities, originally initiated with the aim to improve supervisory convergence. This led to some proposals from a regulatory perspective.

EIOPA has continued its prudential oversight work during 2020 and strengthened its oversight activities on conduct of business, initiating also in this area bilateral visits to National Competent Authorities (NCAs).

Furthermore, EIOPA has continued its activity to increase the level of supervisory convergence in the area of internal model, including – among others - its consistency projects with a view of tackling some aspects of the calibration of internal model.

Following up the change of EIOPA's regulation, EIOPA has prepared to assist NCAs, upon request, handling requests for new approvals of internal model or model changes.

Since the introduction of this new task, no request for assistance has yet been submitted to EIOPA.

Sound supervision of cross border activities, be it under free provision of services or the right of establishment, has emerged as a compelling priority to enhance trust of consumers in the wellfunctioning of the internal market.

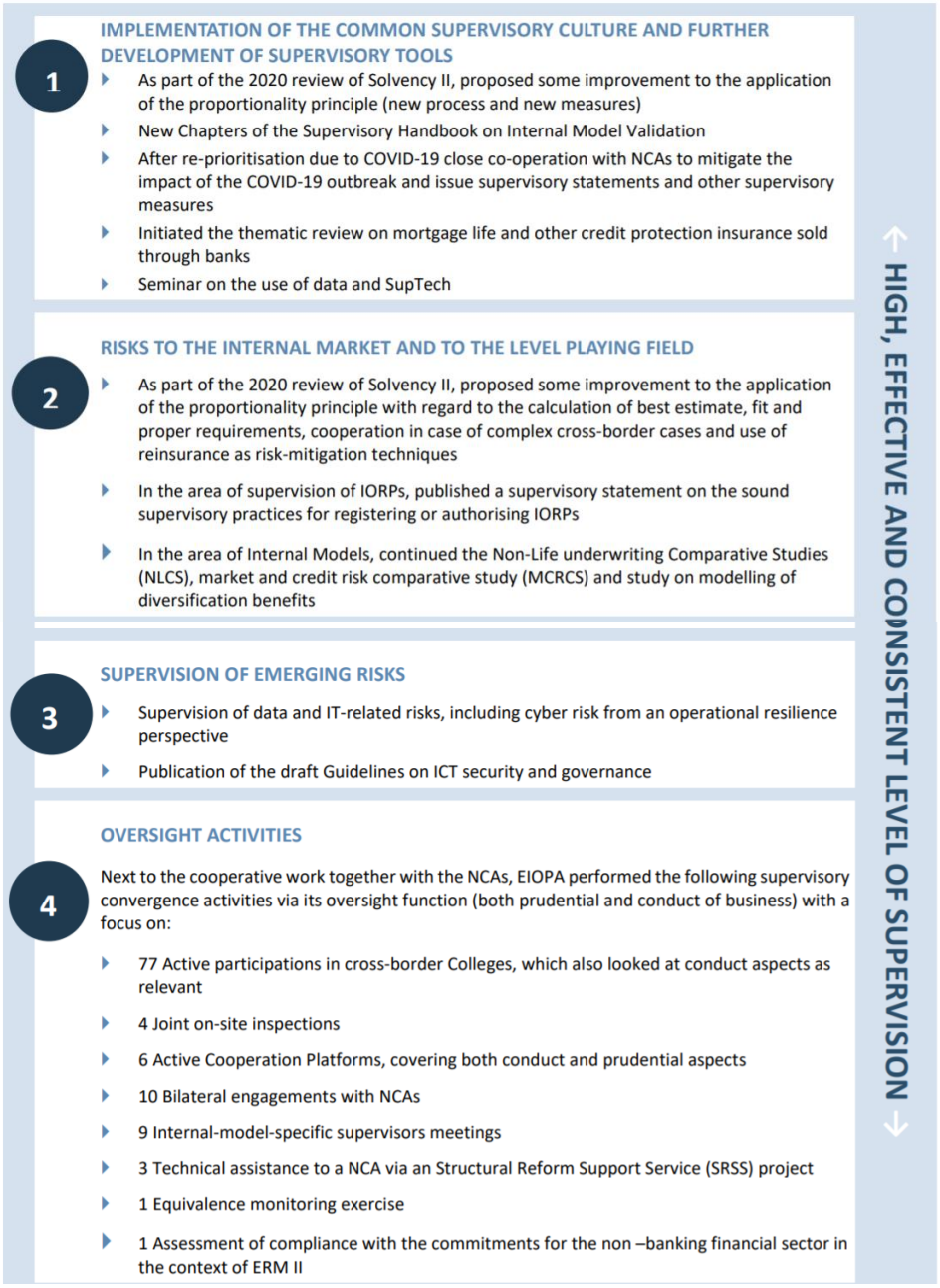
By the end of 2020, six cooperation platforms were operational with the involvement of 21 NCAs.

The cooperation platforms are active as long as the risks identified raise concerns about the appropriate level of protection of policyholders.

Many actions and measures were taken and implemented in 2020 with the aim to conduce to timely supervisory actions to the benefit of consumers.

For some of the platforms the intensive cooperation is continuing into 2021.

Figure 1 presents an overview of the activities EIOPA developed in 2020 to strengthen supervisory convergence in more detail:



To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_bos-21-097-report-on-supervisory-activities.pdf

EBA consults on new Guidelines on the role of AML/CFT compliance officers

The European Banking Authority (EBA) has launched a public consultation on new Guidelines on the role, tasks and responsibilities of anti-money laundering and countering the financing of terrorism (AML/CFT) compliance officers.

The Guidelines also include provisions on the wider AML/CFT governance set-up, including at the level of the group. Once adopted, these Guidelines will apply to all financial sector operators that are within the scope of the AML Directive.

This consultation runs until **2 November 2021.**

The draft Guidelines comprehensively address, for the first time at the level of the EU, the whole AML/CFT governance set-up.

They set clear expectations of the role, tasks and responsibilities of the AML/CFT compliance officer and the management body and how they interact, including at group level.

AML/CFT compliance officers need to have a sufficient level of seniority, which entails the powers to propose, on their own initiative, all necessary or appropriate measures to ensure the compliance and effectiveness of the internal AML/CFT measures to the management body in its supervisory and management function.

Without prejudice to the overall and collective responsibility of the management body, the draft Guidelines also specify the tasks and role of the member of the management board, or the senior manager where no management board exists, who are in charge of AML/CFT overall, and on the role of group AML/CFT compliance officers.

As information reaching the management body needs to be sufficiently comprehensive to enable informed decision-making, the draft Guidelines set out which information should be at least included in the activity report of the AML/CFT compliance officer to the management body.

Where a financial services operator is part of a group, the draft Guidelines provide that a Group AML/CFT compliance officer in the parent company should be appointed to ensure the establishment and implementation of effective group-wide AML/CFT policies and procedures and to ensure that

any shortcomings in the AML/CFT framework affecting the entire group or a large part of the group are addressed effectively.

Provisions in the draft Guidelines are designed to be applied in a proportionate manner, taking into account the diversity of financial sector operators that are within the scope of the AML Directive.

They are also in line with existing ESA guidelines, in particular:

- the revised Guidelines on internal governance under the capital requirements Directive (CRD);

- the revised Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body;

- the draft Guidelines on the authorisation of credit institutions; and

- the draft Guidelines for common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing.

Consultation process

Comments to the draft Guidelines can be sent by clicking on the "send your comments" button on the EBA's consultation page. The deadline for the submission of comments is 2 November 2021.

All contributions received will be published following the close of the consultation, unless requested otherwise.

The EBA will hold a virtual public hearing on the draft Guidelines on 28 September 2021 from 10:00 to 12:00 Paris time. The dial-in details will be communicated to those who have registered for the meeting.

Legal basis and background

The EBA drafted these Guidelines in line with its legal mandate to lead, coordinate and monitor the EU financial sector's fight against ML/TF.

In drafting these guidelines, the EBA fulfills a request by the Commission's request in its Supra-National Risk Assessment (SNRA) of 2019 to develop guidance that 'clarifies the role of AML/CFT compliance officers in credit and financial institutions'.

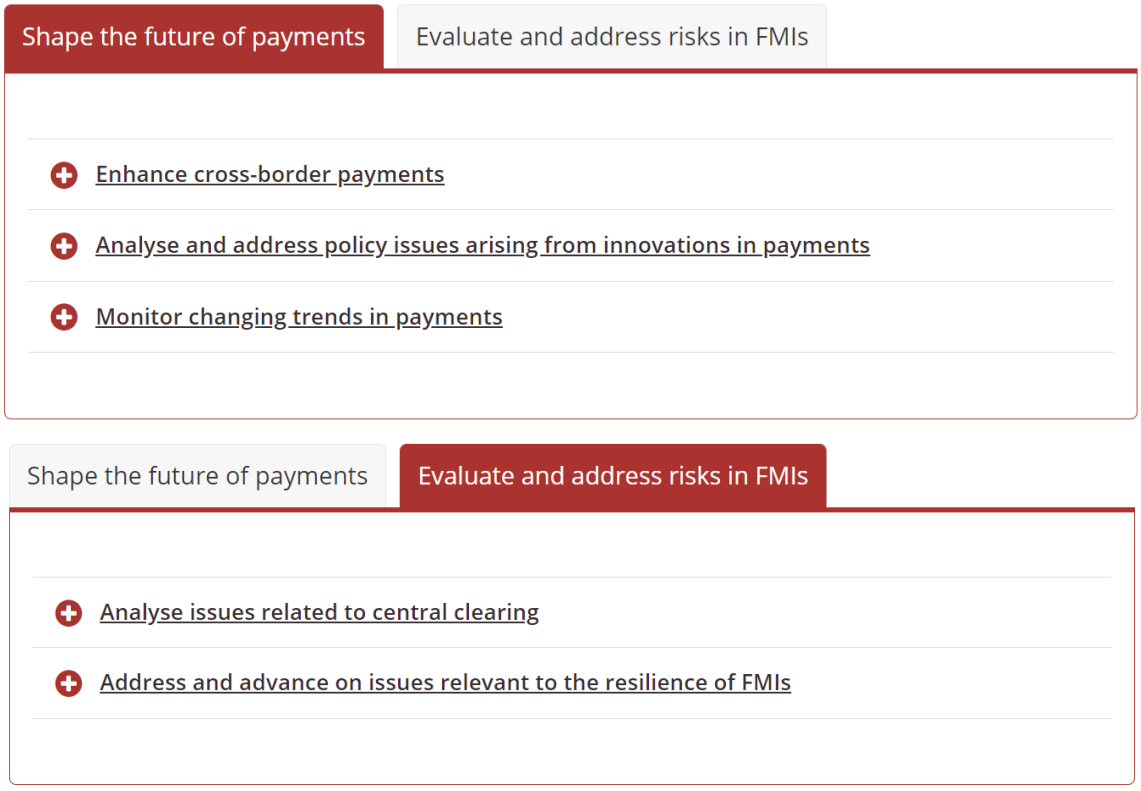
To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2021/Consultation%20on%20draft%20Guidelines%20on%20the%20role%2C%20tasks%20and%20responsibilities%20AML-CFT%20compliance%20officers/1018277/CP%20GLs%20on%20AMLCFT%20compliance%20officer.pdf

Committee on Payments and Market Infrastructures publishes work programme for 2021-22

- Committee on Payments and Market Infrastructures (CPMI) publishes its work programme for the first time.

- The 2021–22 work programme focuses on shaping the future of payments and addressing risks in financial market infrastructures.

- CPMI's priorities include: enhancing cross-border payments; addressing policy issues arising from innovations in payments; evaluating and addressing risks in financial market infrastructures that emerged or were accentuated during the pandemic.



The CPMI has published its work programme for 2021–22, which will focus on shaping the future of payments and addressing risks in financial market infrastructures.

The annual work programme has been publicly released for the first time as part of the CPMI's commitment to increased transparency.
The work programme outlines the strategic priorities for its monitoring and analysis, policy, and standard-setting and implementation activities, under its two overarching themes:

Shaping the future of payments will include enhancing cross-border payments and addressing policy issues arising from digital innovations in payments (such as central bank digital currencies and stablecoins), while monitoring changing trends in payments.

Evaluating and addressing risks in financial market infrastructures will work on issues related to central clearing and others that emerged or were accentuated over the course of the Covid-19 pandemic.

The programme was drawn up under the direction of CPMI Chair Sir Jon Cunliffe in consultation with the Governors of the BIS Economic Consultative Committee.

About the Committee's work

The CPMI carries out its mandate through the following activities:

- monitoring and analysing developments to help identify risks for the safety and efficiency of arrangements within its mandate as well as resulting risks for the global financial system;

- sharing experiences related to arrangements within its mandate, to the performance of oversight functions and to the provision of central bank services in order to promote common understanding, and developing policy advice or common policies for central banks;

- establishing and promoting global standards and recommendations for the regulation, oversight and practices of arrangements within its mandate, including guidance for their interpretation and implementation, where appropriate;

- monitoring the implementation of CPMI standards and recommendations with the purpose of ensuring timely, consistent and effective implementation;

- supporting cooperative oversight and cross-border information-sharing, including crisis communication and contingency planning for cross-border crisis management;

- maintaining relationships with central banks which are not members of the CPMI to share experiences and views and to promote the implementation of CPMI standards and recommendations beyond CPMI member jurisdictions, either directly or by supporting regional bodies as appropriate; and

- coordinating and cooperating with other financial sector standard setters, central bank bodies and international financial institutions.

To read more: https://www.bis.org/cpmi/cpmi_work.htm

NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

When it comes to passwords, the challenges are endless. We must create multiple passwords to manage our many online accounts, from email to shopping sites and social media profiles.

We have to safely keep track of these many passwords and ensure they're strong enough to reduce the risk of cyberattacks.

All of these reasons emphasize why education and training are so important for strengthening passwords and protecting personal accounts.

The problem isn't limited to just adults. Children may seem more technologically savvy because they've grown up in the digital space, but they still face the same cybersecurity threats.

So, to shed light on what kids understand about passwords and their behavior in creating and using them, researchers at the National Institute of Standards and Technology (NIST) conducted a study that surveyed kids from third to 12th grade.

The study found that children are learning best practices, such as memorizing passwords, but are demonstrating a gap between their knowledge of good password practices and their behavior.

The NIST researchers present their findings today at a virtual cybersecurity conference called USENIX Security Symposium 2021.

According to recent data from the Pew Research Center, more than one-third of parents with a child younger than 12 say their child began interacting with a smartphone before the age of 5, and 67% of parents say their child uses or interacts with a tablet computer. You may visit: https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

"Younger children rely on parents a lot. Their first passwords were either given to them at school or by a parent to open their phone or tablet. So, what kind of guidance can we provide?" said NIST researcher Yee-Yin Choong.

The researchers surveyed more than 1,500 kids from ages 8 to 18 who attended schools across the South, Midwest and Eastern regions of the U.S.

Teachers administered two versions of the survey, one for third to fifth graders and the other for sixth to 12th graders. Each survey featured the same questions but had different age-appropriate language.

On the plus side, results from the study showed that kids are learning best practices on passwords, such as limiting their writing of passwords on paper, keeping their passwords private, and logging out after online sessions. They're also not burdened with a lot of passwords as adults are, with kids on average reporting they have two passwords for school and two to four for home.

The passwords that kids created often consisted of concepts reflecting the current state of their lives. Passwords referenced sports, video games, names, animals, movies, titles (such as "princess"), numbers and colors. Examples included "yellow," "doggysafesecure" and "PrincessFrog248."

Password strength increased from elementary to high school students. Examples of stronger passwords among middle and high school students included "dancingdinosaursavrwhoop164" and "Aiken_bacon@28."

But despite the evidence that kids are learning best practices, they also demonstrated bad password habits. They tended to reuse passwords, a habit that increased in frequency from elementary to high school students, and shared their passwords with their friends. "For adolescents, an important part of building friendships is building trust, which is shown with sharing secrets. Their perspective is that sharing passwords is not risky behavior," said Choong.

The study also shed light onto what kids thought about passwords. The survey asked, "Why do people need passwords?" The answers were different for younger and older kids. Elementary students said safety was the primary reason, while for middle and high school students, privacy became more a more dominant answer.

Another notable finding was that younger kids relied on family support for creating and maintaining their passwords at home. This suggests that families play a central role in establishing best practices and that parents affect kids' behavior with passwords.

Not many studies have been performed on kids and cybersecurity, said Choong, which is why this work could be significant in helping researchers understand more about kids' password use.

"This was a very carefully designed study. We had to think carefully about the methodology," said Choong. Researchers contacted the principal of each school first to gain school support for the research, she said. They also

worked with the teachers in getting parental consent and administering the surveys.

In future work, the NIST researchers will move outside the scope of passwords to investigate children's and parents' perceptions of online security, privacy and risky behaviors.

"The end goal of this research is to better support children and provide recommendations that can be used to provide guidance to them, parents and educators. Overall, the focus is on providing guidelines and best practices so that they can stay safe and secure online while enjoying the benefits of the internet," said Choong.

Attackers use Morse code, other encryption methods in evasive phishing campaign

Microsoft 365 Defender Threat Intelligence Team

Cybercriminals attempt to change tactics as fast as security and protection technologies do. During our year-long investigation of a targeted, invoice-themed XLS.HTML phishing campaign, attackers changed obfuscation and encryption mechanisms every 37 days on average, demonstrating high motivation and skill to constantly evade detection and keep the credential theft operation running.

This phishing campaign exemplifies the modern email threat: sophisticated, evasive, and relentlessly evolving.

The HTML attachment is divided into several segments, including the JavaScript files used to steal passwords, which are then encoded using various mechanisms.

These attackers moved from using plaintext HTML code to employing multiple encoding techniques, including old and unusual encryption methods like Morse code, to hide these attack segments.

Some of these code segments are not even present in the attachment itself. Instead, they reside in various open directories and are called by encoded scripts.

In effect, the attachment is comparable to a jigsaw puzzle: on their own, the individual segments of the HMTL file may appear harmless at the code level and may thus slip past conventional security solutions. Only when these segments are put together and properly decoded does the malicious intent show.

This campaign's primary goal is to harvest usernames, passwords, and—in its more recent iteration—other information like IP address and location, which attackers use as the initial entry point for later infiltration attempts.

As we previously noted, the campaign components include information about the targets, such as their email address and company logo. Such details enhance a campaign's social engineering lure and suggest that a prior reconnaissance of a target recipient occurs.

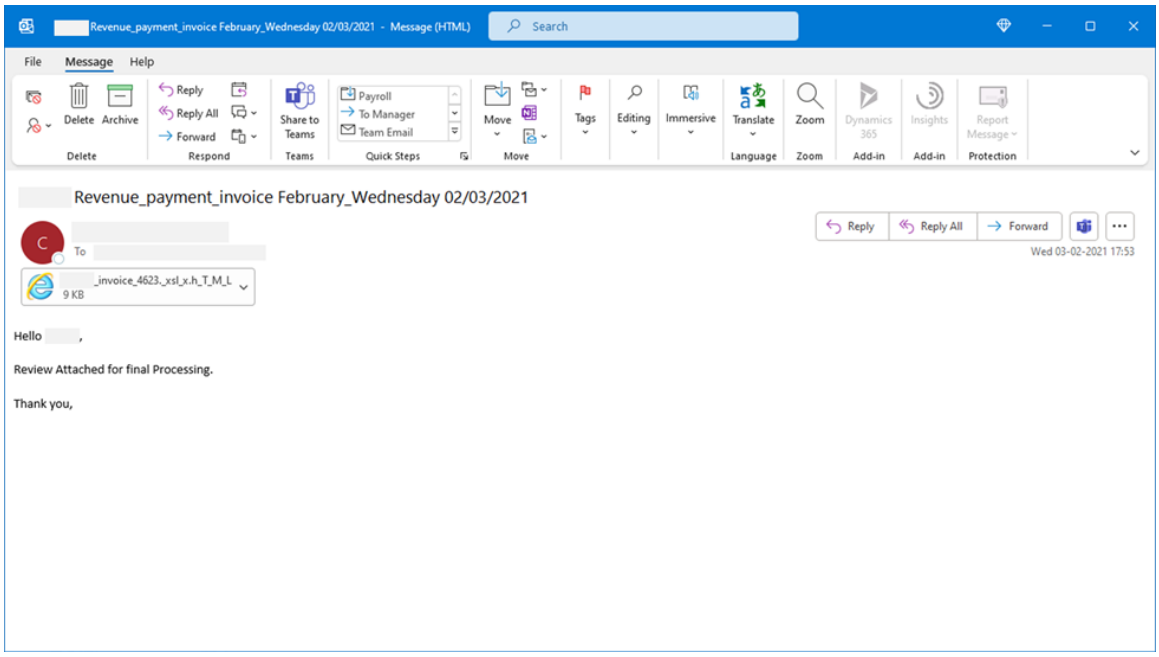
Email-based attacks continue to make novel attempts to bypass email security solutions. In the case of this phishing campaign, these attempts include using multilayer obfuscation and encryption mechanisms for

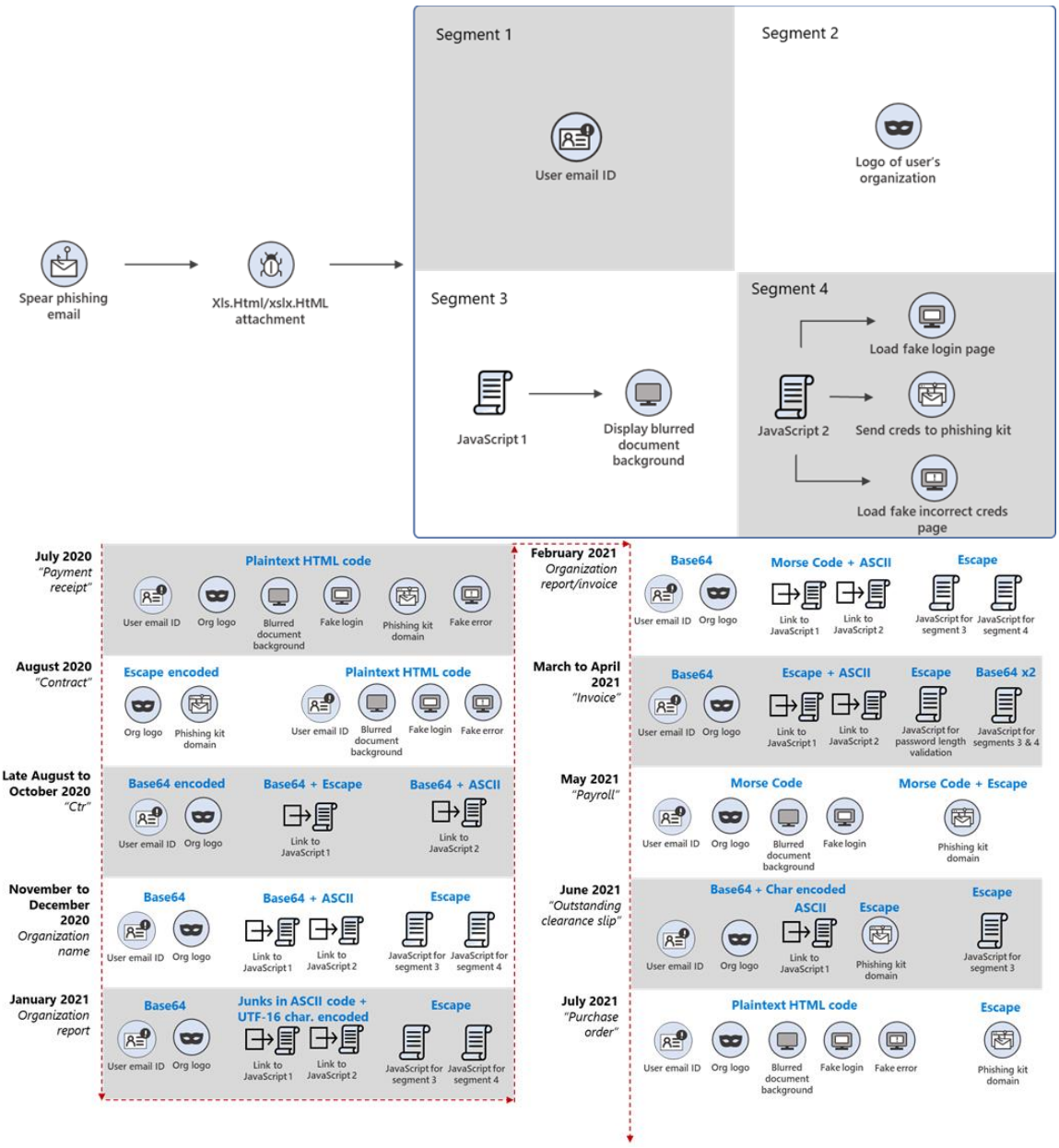
known existing file types, such as JavaScript. Multilayer obfuscation in HTML can likewise evade browser security solutions.

To defend organizations against this campaign and similar threats, Microsoft Defender for Office 365 uses multiple layers of dynamic protection technologies backed by security expert monitoring of email campaigns.

Rich email threat data from Defender for Office 365 informs Microsoft 365 Defender, which provides coordinated defense against follow-on attacks that use credentials stolen through phishing.

Microsoft 365 Defender does this by correlating threat data from email, endpoints, identities, and cloud apps to provide cross-domain defense.





To read more:
https://www.microsoft.com/security/blog/2021/08/12/attackers-use-morse-code-other-encryption-methods-in-evasive-phishing-campaign/

Enabling Military Systems to Adapt to the Unexpected

Program aims to provide physical systems with ability to adapt to unexpected events in real-time and effectively communicate system changes to human and AI operators

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Many complex, cyber-physical military systems are designed to last for decades but their expected functionality and capabilities will likely evolve over time, prompting a need for modifications and adaptation.

High Mobility Multipurpose Wheeled Vehicles (HMMWV), for example, had a design life of 15 years, but are now undergoing modernization to extend the average age of the fleet to 37+ years.

At design time, these systems are built to handle a range of expected operating environments and parameters.

Adapting them is currently done in an improvisational manner – often involving custom-tailored aftermarket remedies, which are not always commonly available, require a skilled technician to install, and can take months or even years to procure.

Further, as they evolve and are placed outside of their original design envelop these systems can fail unexpectedly or become unintentionally dangerous.

"Today, we start with exquisitely built control systems but then someone needs to add something or make a modification – all of which results in changes to the safe operating limits," said DARPA program manager John-Francis Mergen. "These changes are done in a way that wasn't anticipated – or more likely couldn't have been anticipated – by the original designers. Knowing that military systems will undoubtedly need to be altered, we need greater adaptability."

In response, DARPA developed the Learning Introspective Control (LINC) program. The program aims to develop machine learning (ML)-based introspection technologies that enable systems to adapt their control laws as they encounter uncertainty or unexpected events.

The program also seeks to develop technologies to communicate these changes to a human or AI operator while retaining operator confidence and ensuring continuity of operations.

"When a system 'wakes up' in a different space, it needs to be able to realize there are things it can't do anymore or new things it can, and 'learn' how to

adapt to its new operating reality," noted Mergen. "With LINC, we want to provide physical systems with the ability to figure out what is still feasible, alert the operator, and then help them operate in that new space."

Developing LINC technologies will require addressing a specific set of challenges related to learning control and communicating situational awareness to the operator.

Current state of the art (SOTA) ML approaches are not robust to unknown or unstructured parameter uncertainty, owing largely to the bounds set on their operation at design time as well as their reliance on fixed assumptions about their operating model.

Further, complex systems – like drone swarms – are unable to rapidly converge on a common solution.

When damage occurs to a single drone, the swarm is unable to uniformly adapt, potentially resulting in a failed operator or unsafe operating conditions.

LINC's first research area will seek to overcome existing limitations in learning models and ML techniques that currently hamper system adaptation.

The program will explore how to provide a system with the ability to sense change and then reconstitute control using only onboard sensors and actuators.

LINC aims to develop new control regimes that detect and characterize changes in the system's operations in real-time, rapidly find solutions for reconstituting control under these changing conditions, and then calculate operating limits to identify a safe operating envelope.

"The idea is that you have a plethora of indigenous sensors on the system, and you can use these to determine and define a new set of control laws. With those new laws, you can then calibrate the system," said Mergen.

Another challenge area LINC seeks to address is around operator communications.

Today, operators are not often provided with sufficient explanations or guidance around a system's behavior or it's situation-specific operating limits. Existing cues to operators about system dynamics don't always provide options, making it difficult for an operator to appropriately trust the information its receiving.

Further, interpreting current system diagnostics displays, which are not always intuitive, creates additional cognitive load for human operators.

This further erodes operator trust and can lead to misunderstanding, confusion, and incorrect actions.

A second research area will focus on improving how situational awareness and guidance are shared with the operator. This area will explore ways of translating and effectively communicating the operational information generated by the dynamic model developed under the first research area.

The resulting technologies must be able to provide the operator – whether human or AI – with updates on the operating status of the system as well as cues for safe actions. Further, they must be able to help retain operator trust by providing optionality and explainability around what's happening "under the hood."

A third research area will focus on testing and evaluating the resulting technologies. LINC expects to use demonstration platforms that will evolve in sophistication and complexity throughout the life of the program – starting with a realistic physical model and progressing to a military-relevant system in the program's final phase.

Interested proposers will have an opportunity to learn more about the Learning Introspective Control (LINC) program during a Proposers Day, which will be held on August 26, 2021, from 9:00 AM to 2:00 PM (ET) both at the DARPA Conference Center, located at 675 N. Randolph Street, Arlington, Virginia, 22203, and virtually through Zoom. Advance registration is required to attend. To learn more: https://sam.gov/opp/69db6bff225344f481f229edc1e2b97a/view

The LINC Broad Agency Announcement is forthcoming and will be published on the System for Award Management (SAM) website at https://beta.sam.gov/

Project Dunbar: international settlements using multi-CBDCs

Project Dunbar brings together the Reserve Bank of Australia, Bank Negara Malaysia, Monetary Authority of Singapore, and South African Reserve Bank with the Bank for International Settlements Innovation Hub to test the use of central bank digital currencies (CBDCs) for international settlements.

Led by our Singapore Centre, it aims to develop prototype shared platforms for cross-border transactions using multiple CBDCs, allowing financial institutions to transact directly with each other in the digital currencies, eliminating the need for intermediaries and cutting the time and cost of transactions.

The project will focus initially on the development of a common platform for multi-CBDC settlement (Model 3 – mCBDC arrangements based on single multi-currency system) that fulfils the needs and requirements of central banks and financial institutions. You may visit: https://www.bis.org/publ/bppdf/bispap115.htm

Table of Contents

Introduction 1

Cross-border payment frictions and interoperability – a primer 2

Cross-border CBDCs: three conceptual approaches 4

Enhancing compatibility of CBDCs 4

Linking multiple CBDC systems 5

Integrating multiple CBDCs in a single mCBDC system 7

International coordination to harness the potential of mCBDC arrangements 9

Compatibility 10

Coordination 11

Concluding thoughts 12

References 14

Previous volumes in this series 17

The project will work with multiple partners to develop technical prototypes on different distributed ledger technology platforms. It will also explore different governance and operating designs that would enable

central banks to share CBDC infrastructures, benefitting from the collaboration between public and private sector experts in different jurisdictions and areas of operation.

This work will explore the international dimension of CBDCs design and support the efforts of the G20 roadmap for enhancing cross-border payments. Its results, expected to be published in early 2022, will inform the development of future platforms for global and regional settlements.

Model Risk Management

Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency's (OCC) Comptroller's Handbook booklet, "Model Risk Management," is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and agencies of foreign banking organizations (collectively, banks).

Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances.

This booklet aligns with the principles laid out in the "Supervisory Guidance on Model Risk Management" conveyed by OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management" (MRM Supervisory Guidance).

This booklet:

• is designed to guide examiners in performing consistent, high-quality model risk management examinations.

• presents the concepts and general principles of model risk management.

• informs and educates examiners about sound model risk management practices that should be assessed during an examination.

• provides information needed to plan and coordinate examinations on model risk management, identify deficient practices, and conduct appropriate follow-up.

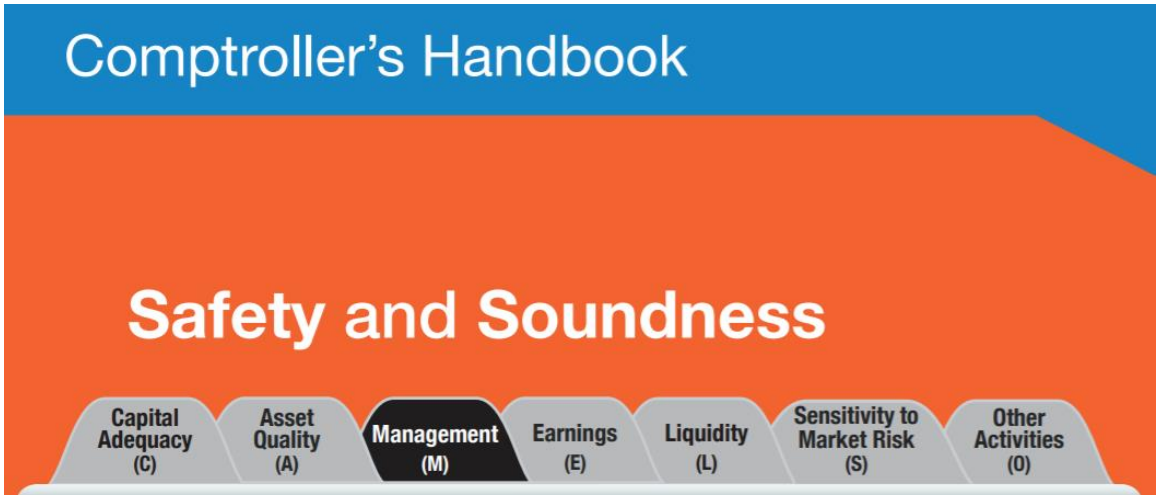
Introduction **1**
Background 1
Risks Associated With the Use of Models 4
Strategic Risk 6
Operational Risk 6
Reputation Risk 7
Compliance Risk 8
Credit Risk 9
Liquidity Risk 9
Interest Rate Risk 10
Price Risk 10

Risk Management **12**
Governance 13
Board and Management Oversight 15
Personnel 16
Model Owners 17
Independent Risk Management Staff 18
Internal Audit 19
Policies and Procedures 21
Risk Assessment 24
Planning 25
Model Inventory 26
Documentation 28
Data Management 29
Model Development, Implementation, and Use 30
Model Development and Implementation 31
Testing 32
Ongoing Development 33
Model Use 33
Model Overlays and Adjustments 34
Reporting 35
Model Validation 36
Evaluation of Conceptual Soundness 39
Ongoing Monitoring 42
Process Verification 43
Benchmarking 44
Outcomes Analysis 45
Back-Testing 47
Third-Party Risk Management 48
Third-Party Models and Data 48
Engaging Third Parties for Model Risk Management Activities 50
IT Systems 51

Examination Procedures **53**
Scope 53
Quantity of Risk 55
Quality of Model Risk Management 58
Conclusions 82
Internal Control Questionnaire 84

Glossary **103**

References **105**



You may visit: https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html

Annual Report on the Interim Inspection Program Related to Audits of Brokers and Dealers - PCAOB Release No. 2021-002

The Public Company Accounting Oversight Board (PCAOB) has registration, inspection, standard-setting, and disciplinary authority over the auditors of brokers and dealers registered with the U.S. Securities and Exchange Commission (SEC).

Overseeing the audits of SEC-registered broker-dealers is a key component of the PCAOB's mission to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports.

This Annual Report on the Interim Inspection Program Related to Audits of Brokers and Dealers ("Annual Report") provides:

(1) information about our 2020 inspections approach,

(2) a summary of our 2020 inspections observations, and

(3) "good practices," which include brief scenarios and possible procedures that may be effective to address those scenarios.

The information in this Annual Report is provided under the requirements of PCAOB Rule 4020T, which addresses reporting under the interim inspection program.

Under Securities Exchange Act of 1934 ("Exchange Act") Rule 17a-5, broker-dealers registered with the SEC are generally required to file annually: a financial report and either a compliance report (if the broker-dealer did not claim it was exempt from Exchange Act Rule 15c3-3, Customer Protection – Reserves and Custody of Securities ("Customer Protection Rule")) or an exemption report (if the broker-dealer did claim it was exempt from the Customer Protection Rule), as well as reports of an independent public accountant covering the financial report and the compliance report or exemption report, as applicable.

The accountant must be engaged to prepare a report based on an examination of the financial report in accordance with PCAOB auditing standards ("audit engagement") and a report based on an examination of certain statements in the compliance report ("examination engagement") or a report based on a review of the exemption report ("review engagement"). The PCAOB has issued attestation standards covering the compliance report (AT No. 1) and the exemption report (AT No. 2).

Overarching observations from our 2020 inspections of firms that audit broker-dealers include the following:

- The number of firms that had one or more audit and/or attestation engagements with deficiencies showed a 14% drop from 2019 but remained high as a percentage of firms inspected (78%).

- The number of audit engagements with deficiencies declined 15% from 2019 levels but remained high as a percentage of engagements reviewed (61%) primarily due to deficiencies in auditing revenue.

- The percentage of examination engagements with deficiencies declined slightly to 67% of engagements reviewed from 69% in 2019 but remained high primarily due to deficiencies in testing internal control over compliance (ICOC). Examination engagements address assertions made by broker-dealers in compliance reports.

- The percentage of review engagements with deficiencies declined to 23% of engagements reviewed from 51% in 2019. Review engagements address assertions made by broker-dealers in exemption reports.

- Generally, the results of inspections of firms that audited more than 100 broker-dealers resulted in lower percentages of audit engagements with deficiencies, compared to the results for firms that audited 100 or fewer broker-dealers. For firms that audited more than 100 broker-dealers, the percentage of audit engagements with deficiencies declined to 38% in 2020 from 41% in 2019. For all other firms, the percentage of audit engagements with deficiencies declined to 71% in 2020 from 84% in 2019.

Additional information about inspection results based on firm characteristics is included in the supplement to this Annual Report.

By highlighting deficiencies and good practices, this Annual Report helps to advance our strategic goal of driving improvement in the quality of audit services through a combination of prevention, detection, deterrence, and remediation.

In addition to being helpful to audit firms, it may also be useful for other stakeholders, including management and the audit committee (or equivalent body) of broker-dealers, as they engage with audit firms regarding audit quality and broker-dealer financial reporting.

Overview 3

2020 Inspections Approach 6

Information About Selected Firms and Engagements 8

Firms 8

Engagements 8

Inspections Observations 11

Deficiencies in Attestation and Audit Engagements 12

Other Instances of Non-Compliance with PCAOB Standards 23

Deficiencies in Quality Control Systems 25

Auditor Independence Findings 26

PCAOB Standards Associated with Inspections Observations 27

Learn More and Provide Feedback 28

To read more: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/inspections/documents/2020-broker-dealer-annual-report.pdf?sfvrsn=d8914df5_4

NCSC and Federal Partners Kick Off "National Insider Threat Awareness Month"

This Year's Campaign Focuses on Insider Threat and Workplace Culture; Marks Nearly 10 Years since Executive Order Creating National Insider Threat Task Force

The National Counterintelligence and Security Center (NCSC), the National Insider Threat Task Force (NITTF), the Office of the Under Secretary of Defense Intelligence and Security, the Defense Counterintelligence and Security Agency, and the Department of Homeland Security today launched the third-annual "National Insider Threat Awareness Month" (NITAM).

NITAM is an annual, month-long campaign during September to educate government and industry about the risks posed by insider threats and the role of insider threat programs.

Federal insider threat programs are composed of multi-disciplinary teams that address insider threats while protecting privacy and civil liberties of the workforce; maximizing organizational trust and ensuring positive work cultures that foster diversity and inclusion.

The NITAM campaign seeks to encourage employees in government and the private sector to recognize behaviors of concern and report them so early intervention can occur, leading to positive outcomes for at-risk individuals and reduced risks to organizations.

To learn more about the campaign and resources available to organizations, visit the NITAM 2021 website. You may visit: https://www.cdse.edu/itawareness/index.html

All organizations are vulnerable to insider threats. An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly harm an organization or its resources.

Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many insider threats can be mitigated before harm occurs.

"The risks to government and industry from insider threats are severe. These threats can take many forms, whether it's a federal employee

coopted by a foreign adversary to steal sensitive information or a corporate employee clicking on a spear-phishing link that infects their company's networks," said NCSC Acting Director Michael Orlando.

"Through this campaign, we hope to bring much-needed attention to insider threats and help organizations and their employees prevent and mitigate these issues early on."

This year's campaign focuses on insider threat and workplace culture. Organizations with positive and inclusive work cultures that foster trust between employees and leadership have more engaged and loyal employees and are better positioned to reduce insider threats.

Studies have demonstrated that disengaged workers have higher absenteeism, more accidents, and more errors, and that organizations with low employee engagement suffer from lower productivity, lower profitability, and lower job growth – all conditions that can contribute to insider threats.

Tomorrow, insider threat practitioners from across the U.S. government and industry will participate in the 2021 Insider Threat Virtual Conference, sponsored by the Department of Defense. You may visit: https://cdse-events.acms.com/content/connect/c1/7/en/events/event/shared/33897197/event_landing.html?sco-id=33880313&_charset_=utf-8

The conference features senior level speakers and panelists who will present on the current state of federal and industry insider threat programs; the importance of and strategies for developing positive organizational culture and sub-culture in combating the insider threat; and resources for training and professionalization of the insider threat practitioner community.

Recent examples underscore the damage that can be caused by insider threats:

- In July 2021, a 20-year-old sailor who had failed in his attempt at becoming a Navy SEAL was charged with deliberately setting fire to the USS Bonhomme Richard, an 800-foot Navy amphibious assault ship. The USS Bonhomme Richard went up in flames on July 12, 2020, burning for several days while docked in San Diego and causing some 60 people to be treated for injuries. The Navy later decided against repairing the vessel after determining it would cost an estimated $3 billion and take more than five years. The Navy officially decommissioned the USS Bonhomme Richard this year.

- In April 2021, a Ph.D. chemist who had worked at Coca-Cola and Eastman Chemicals was convicted of conspiracy to steal trade secrets, economic espionage, and wire fraud. According to court documents, the chemist stole trade secrets that cost some $120 million to develop in order to help a new company in China that had received millions of dollars in grants from the Chinese government. The chemist sought to benefit not only the Chinese company, but also the Chinese government and Communist Party.

The launch of this year's campaign marks nearly a decade since an October 2011 Executive Order that required all federal agencies with access to classified information to have their own insider threat prevention programs and directed the creation of the NITTF under the leadership of the Attorney General and the Director of National Intelligence.

NITTF is currently housed at NCSC. Since its inception, the NITTF has worked with federal agencies to build programs that deter, detect, and mitigate insider threats.

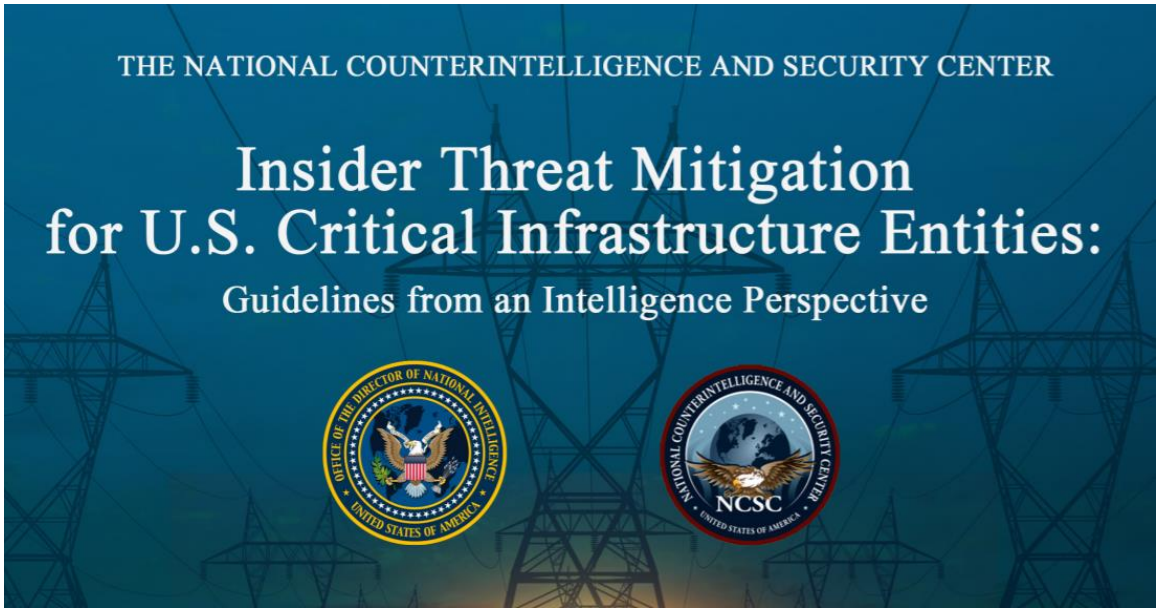
NITTF and NCSC coordinate insider threat training and awareness; liaison and assistance; governance and advocacy; and research and analysis for stakeholders in the public and private sector to reduce the risk of insider threats to public health and safety, economic security, and national security.

In recent years, NCSC and NITTF have expanded their outreach to help private sector entities address insider threats.

In March 2021, NCSC published Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective, and in July 2021, NCSC and the Department of Defense's Center for Development of Security Excellence (CDSE) collaborated to publish Insider Risk Implementation Guide for the Food and Agriculture Sector.

You may visit:
https://www.dni.gov/files/NCSC/documents/nittf/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021updated-5Apr21b.pdf

https://www.dni.gov/files/NCSC/documents/nittf/Insider_Risk_Implementation_Guide_for_Food_and_Agriculture20210708.pdf


THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
Insider Threat Mitigation
for U.S. Critical Infrastructure Entities:
Guidelines from an Intelligence Perspective
NCSC

Insider Risk Mitigation Programs
Food and Agriculture Sector
Implementation Guide
NCSC

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

International Association of Hedge Funds Professionals (IAHFP)

At every stage of your career, our community provides training, certification programs, resources, updates, networking and services you can use.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit:
https://www.hedge-funds-association.com/HowToBecomeMember.html

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

3. Training and Certification – You may visit:
https://www.hedge-funds-association.com/Distance_Learning_and_Certification.htm