International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, January 30, 2023

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

The law is (and always has been) made by humans for humans, but this is going to change. The rise of Artificial Intelligence (AI) and robots leads to the emergence of *'robot law'*. This is not a joke.

AI is changing the way we live and work. Routine tasks, not only manual but also cognitive, are becoming increasingly automated, and "embodied AI" (robots that use AI to interact with the physical world and to learn from their interactions) take more and more jobs month after month.

Embodied AI is not recognized by law as a natural person, but corporations are not natural persons too. Corporations are legal persons, and have the ability to transact and follow rules, they have obligations, and are liable for certain behaviour. Will robots have a legal personality, like corporations? Will humans that incorporate elements of machine intelligence into their brains and bodies still be considered as natural persons?

Scientists from areas as diverse as law, engineering, philosophy, psychology, sociology, computer science, biology, neuroscience, biomechanics, material science, and linguistics have to work hard to understand the benefits of AI, and to reduce the negative consequences.

A picture may sometimes be worth a thousand words, but a thousand pictures cannot represent what we may mean using a single word. The road is not going to be easy.

Read more about AI developments in Number 1 and 2 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 5)

NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence

New guidance seeks to cultivate trust in AI technologies and promote AI innovation while mitigating risk.

Number 2 (Page 9)

VIDEO: A New Generation of AI Assistants

Perceptually-enabled Task Guidance prototypes demonstrated ability to help people complete recipes as a proxy to unfamiliar tasks

Number 3 (Page 11)

Exploring multilateral platforms for cross-border payments

Number 4 (Page 15)

Implementation of G20 Non-Bank Financial Intermediation Reforms, Progress report

Number 5 (Page 17)

Daring to know in times of uncertainty and structural shifts

Klaas Knot, President of the Netherlands Bank and Chair of the Financial Stability Board, at the 11th ILF Conference on the Future of the Financial Sector "The Next Systemic Financial Crisis – Where Might it Come From?": Financial Stability in a Polycrisis World, at the Goethe University's Law and Finance Institute, Frankfurt am Main.

Number 6 (Page 25)

SEC Proposes Rule to Prohibit Conflicts of Interest in Certain Securitizations

Number 7 (Page 27)

New challenges in a changing world

Christine Lagarde, President of the European Central Bank, at the Deutsche Börse Annual Reception, Eschborn.

Number 8 (Page 29)

Statement on Prohibiting Conflicts of Interest in Securitizations

Chair Gary Gensler, Chair of the U.S. Securities and Exchange Commission

Number 9 (Page 31)

Ransomware-as-a-service (RaaS) - Cybercriminals stung as HIVE infrastructure shut down

Number 10 (Page 35)

U.S. Department of Justice Disrupts Hive Ransomware Variant

FBI Covertly Infiltrated Hive Network, Thwarting Over $130 Million in Ransom Demands

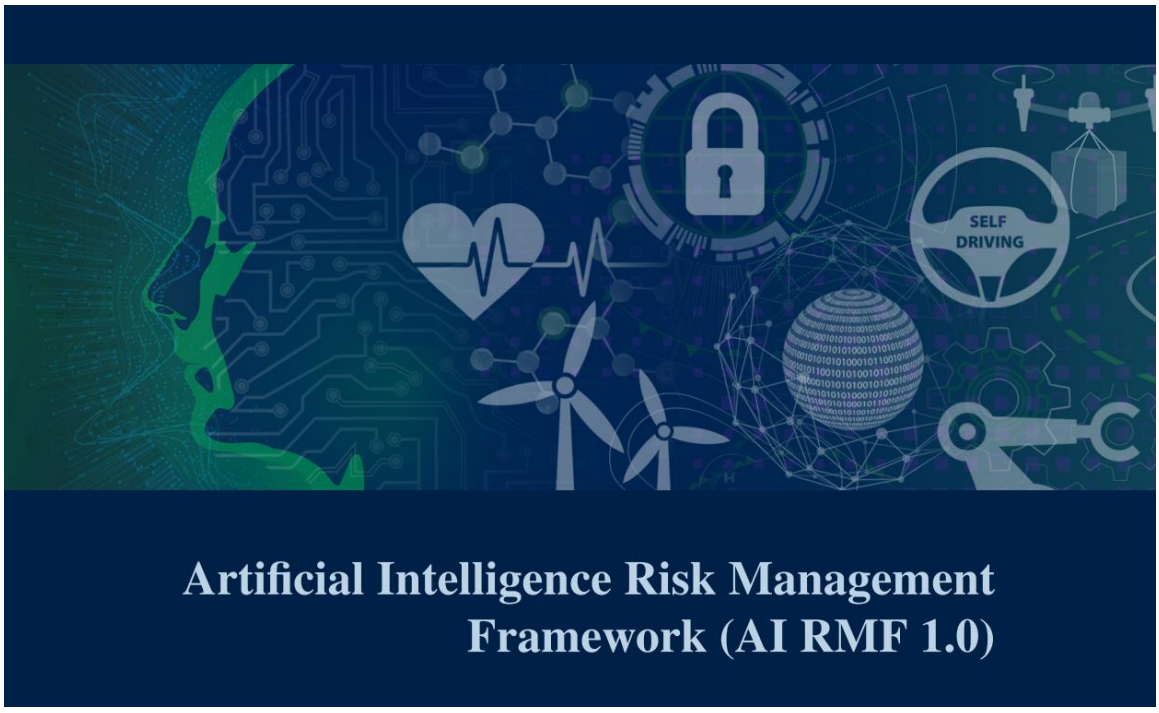
Number 1

NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence

New guidance seeks to cultivate trust in AI technologies and promote AI innovation while mitigating risk.

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

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has released its Artificial Intelligence Risk Management Framework (AI RMF 1.0), a guidance document for voluntary use by organizations designing, developing, deploying or using AI systems to help manage the many risks of AI technologies.



> The AI RMF refers to an *AI system* as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy (Adapted from: OECD Recommendation on AI:2019; ISO/IEC 22989:2022).

The AI RMF follows a direction from Congress for NIST to develop the framework and was produced in close collaboration with the private and public sectors. It is intended to adapt to the AI landscape as technologies

continue to develop, and to be used by organizations in varying degrees and capacities so that society can benefit from AI technologies while also being protected from its potential harms.

“This voluntary framework will help develop and deploy AI technologies in ways that enable the United States, other nations and organizations to enhance AI trustworthiness while managing risks based on our democratic values,” said Deputy Commerce Secretary Don Graves. “It should accelerate AI innovation and growth while advancing — rather than restricting or damaging — civil rights, civil liberties and equity for all.”

Compared with traditional software, AI poses a number of different risks. AI systems are trained on data that can change over time, sometimes significantly and unexpectedly, affecting the systems in ways that can be difficult to understand.

These systems are also “socio-technical” in nature, meaning they are influenced by societal dynamics and human behavior. AI risks can emerge from the complex interplay of these technical and societal factors, affecting people’s lives in situations ranging from their experiences with online chatbots to the results of job and loan applications.

The framework equips organizations to think about AI and risk differently. It promotes a change in institutional culture, encouraging organizations to approach AI with a new perspective — including how to think about, communicate, measure and monitor AI risks and its potential positive and negative impacts.

The AI RMF provides a flexible, structured and measurable process that will enable organizations to address AI risks. Following this process for managing AI risks can maximize the benefits of AI technologies while reducing the likelihood of negative impacts to individuals, groups, communities, organizations and society.

The framework is part of NIST’s larger effort to cultivate trust in AI technologies — necessary if the technology is to be accepted widely by society, according to Under Secretary for Standards and Technology and NIST Director Laurie E. Locascio.

“The AI Risk Management Framework can help companies and other organizations in any sector and any size to jump-start or enhance their AI risk management approaches,” Locascio said. “It offers a new way to integrate responsible practices and actionable guidance to operationalize trustworthy and responsible AI. We expect the AI RMF to help drive development of best practices and standards.”

The AI RMF is divided into two parts. The first part discusses how organizations can frame the risks related to AI and outlines the characteristics of trustworthy AI systems. The second part, the core of the framework, describes four specific functions — govern, map, measure and manage — to help organizations address the risks of AI systems in practice. These functions can be applied in context-specific use cases and at any stages of the AI life cycle.

Working closely with the private and public sectors, NIST has been developing the AI RMF for 18 months. The document reflects about 400 sets of formal comments NIST received from more than 240 different organizations on draft versions of the framework. NIST today released statements from some of the organizations that have already committed to use or promote the framework.

The agency also today released a companion voluntary AI RMF Playbook, which suggests ways to navigate and use the framework.

NIST plans to work with the AI community to update the framework periodically and welcomes suggestions for additions and improvements to the playbook at any time. Comments received by the end of February 2023 will be included in an updated version of the playbook to be released in spring 2023.

To read more:
https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

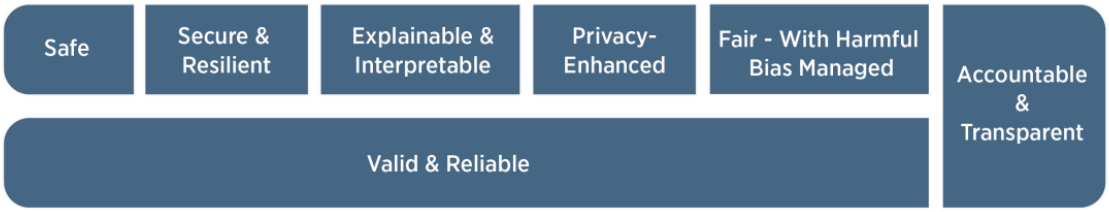


Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

Number 2

VIDEO: A New Generation of AI Assistants

Perceptually-enabled Task Guidance prototypes demonstrated ability to help people complete recipes as a proxy to unfamiliar tasks

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this video, DARPA program manager Dr. Bruce Draper describes the technology he thinks could usher in the next "do-it-yourself" revolution.

The Perceptually-enabled Task Guidance (PTG) program aims to develop virtual "task guidance" assistants that can work with different sensor platforms to help military personnel perform complex physical tasks and expand their skillsets.

Unlike today's AI assistants, PTG technology would be able to see what the user sees and hears what they hear by integrating with a microphone, a head-mounted camera, and displays like augmented reality (AR) headsets, to deliver accurate instructions.

The video: https://www.youtube.com/watch?v=pEM8gcRkA7M

PTG performers* recently demonstrated early successes of their prototypes by using the task of cooking recipes as a proxy for unfamiliar, more complex tasks, such as battlefield medical procedures, military equipment sustainment, and co-piloting aircraft.

*PTG Performers: Kitware (Columbia University; University of California, Berkeley; University of Texas at Austin); PARC (University of California, Santa Barbara; University of Rostock); Northeastern University (University of California, Santa Barbara; Stony Brook University); New York University; University of Texas at Dallas (University of California, Irvine; University of Florida); Stevens Institute of Technology (Purdue University; University of Michigan; University of Rochester); University of Florida (Northeastern University; Topos Institute; Texas A&M University; University of Arizona); Raytheon Technologies (Valkyries Austere Medical Solutions); Northrop Grumman (University of Central Florida); Red Shred (Third Insight); MIT Lincoln Laboratory

“Today the commercial sector is pursuing new, useful ways to present data to the user but it doesn’t go far enough,” said Draper. “The gamechanger with PTG would be having perceptually-driven AI interfaces that can make sense of the real world, react to whatever the user is doing and provide advice. I'm really impressed at how quickly performing teams are making progress toward the goals.”

To read more: https://www.darpa.mil/news-events/2023-01-25

Number 3

Exploring multilateral platforms for cross-border payments

This report provides an assessment of whether and how multilateral platforms could bring meaningful improvements to the cross-border payments ecosystem.

It was written by the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) in collaboration with the BIS Innovation Hub, the International Monetary Fund (IMF) and the World Bank.

The report analyses the potential costs and benefits of these platforms and how they might alleviate some of the cross-border payment frictions. It also evaluates the risks, barriers and challenges to establishing multilateral platforms and explores two paths for their evolution.

The analysis is based on a stocktake, conducted by the CPMI, of existing and potential multilateral platforms as well as bilateral discussions with existing platform operators.

A multilateral platform is a payment system for cross-border payments that is multi-jurisdictional by design. It can substitute for or operate alongside traditional correspondent banking relationships or bilateral interlinking of domestic payment infrastructures.

A multilateral platform can potentially shorten transaction chains by allowing participants in different jurisdictions to send or receive payments directly instead of via multiple intermediaries.

Depending on its design, a platform can offer extended operating hours to meet the requirements of participants in different time zones and ease compliance checks related to anti-money laundering and combating the financing of terrorism (AML/CFT).

Built as new, it can also reduce dependencies on legacy systems by implementing the latest technology and payment message standards.

To the extent a multilateral platform is able to mitigate these underlying frictions, it could reduce the costs and increase the safety, speed and transparency of cross-border payments.

Multilateral platforms could enhance cross-border payments but often involve more complicated legal and operational issues relative to domestic payment systems.

Any decision to increase the role of multilateral platforms should weigh all relevant trade-offs, risks and benefits relative to other cross-border arrangements such as correspondent banking, not merely the added risks relative to domestic systems.

These considerations vary depending on the current state of cross-border payment arrangements in a specific geographical region or for a specific payment system function, as well as on the purpose and chosen approach for increasing the role of multilateral platforms.

The actual improvements that a potential platform can bring to the cross-border payments ecosystem will, of course, depend on its concrete design. Hence, this report can only offer some high-level considerations, without pre-empting potential future considerations on individual business cases.

This report explores two conceptual implementation approaches: the growth approach and the greenfield approach.

The growth approach involves expanding existing multilateral platforms to additional jurisdictions, currencies and participants (including by extending access to foreign participants and interlinking with domestic systems and other platforms).

This option could be based on existing institutional arrangements but may nevertheless require additional public-private sector involvement and coordination.

The greenfield approach involves building a new, potentially global infrastructure for crossborder payments.

This option could foster greater alignment of certain aspects of cross-border payments but may entail complex governance discussions and cooperative oversight arrangements as well as careful balancing of the roles of public and private sector stakeholders.

Policymakers have different options to consider as they analyse the potential development and implementation of multilateral platforms.

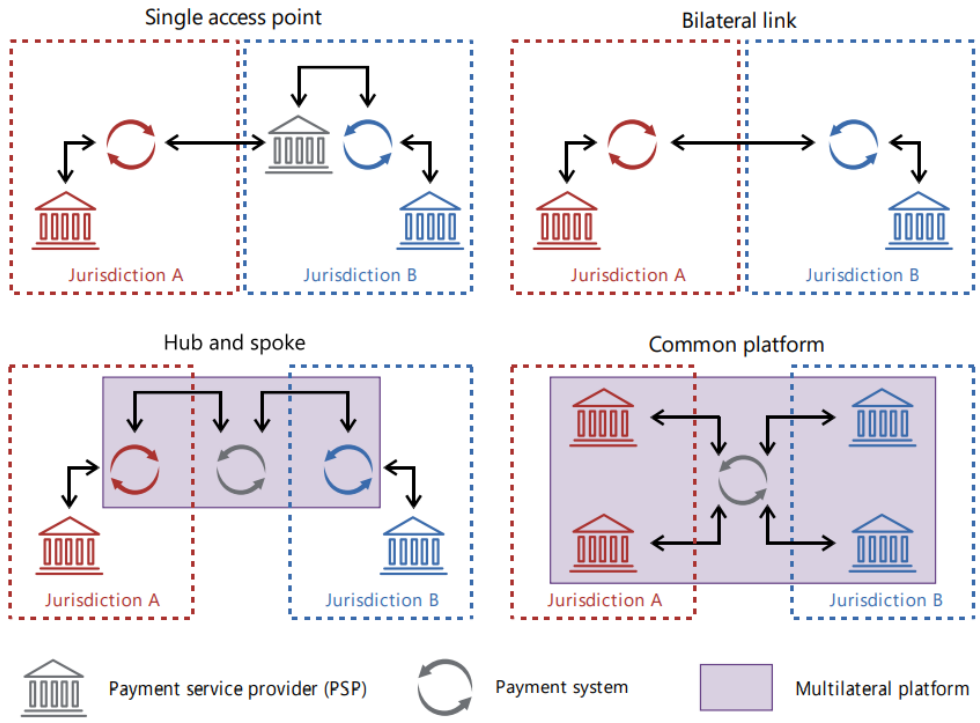
Any evaluation should carefully consider the trade-offs of multilateral platforms and account for the evolving nature of the cross-border payments

market. To this end, possible further measures could entail efforts by regional bodies, operators and/or international organisations to realise the potential of multilateral platforms.

Taking advantage of the momentum generated by the G20 cross-border payments programme, payment system operators and authorities contemplating the expansion or establishment of multilateral platforms can use this analysis as a basis for evaluating the best approach for their specific circumstances. Such preparatory steps could allow relevant stakeholders to gain a sound basis from which to plan and assess future actions.

Contents

Stylised models for interlinking cross-border payment systems[1, 2] Graph 1



[1] Examples include euroSIC (single access point), Directo a México (bilateral link), the Regional Payment and Settlement System (REPSS) of the Common Market for Eastern and Southern Africa (hub and spoke) and Southern African Development Community (SADC)-RTGS (common platform). [2] The multilateral platform includes the participants and the entity operating the arrangement. In the hub and spoke model, the participants are payment systems. In the common platform model, the participants are PSPs.

Source: Adapted from CPMI (2022d).

To read more: https://www.bis.org/cpmi/publ/d213.pdf

Number 4

Implementation of G20 Non-Bank Financial Intermediation Reforms, Progress report

FSB FINANCIAL STABILITY BOARD

This report describes progress in implementing reforms that had been agreed by the G20 following the 2008 global financial crisis to strengthen the oversight and regulation of non-bank financial intermediation (NBFI). The implementation status in various NBFI areas is as follows:

1. Jurisdictions have made progress in implementing Basel III reforms to mitigate spillovers between banks and non-bank financial entities, but implementation is not yet complete.

Four jurisdictions have yet to implement applicable risk-based capital requirements for banks' investments in the equity of funds or the supervisory framework for measuring and controlling banks' large exposures.

2. Adoption of the 2012 IOSCO recommendations to reduce the run risk of money market funds (MMFs) is most advanced in the largest MMF markets.

All FSB members adopted the fair value approach for valuation of MMF portfolios, though one jurisdiction does not have in place requirements for use of the amortised cost method only in limited circumstances.

Progress in liquidity management is less advanced. An IOSCO review found that the policy measures in nine jurisdictions representing about 95% of global net MMF assets are generally in line with the IOSCO recommendations.

3. Adoption of the IOSCO recommendations on incentive alignment approaches for securitisation and of the BCBS standard on revised securitisation framework is ongoing.

About one-third of FSB jurisdictions (for the IOSCO recommendations) and one-sixth of FSB jurisdictions (for the BCBS standard) have yet to implement them.

4. Implementation of FSB recommendations for dampening procyclicality and other financial stability risks associated with securities financing transactions (SFTs) is incomplete and continues to face significant delays in

most jurisdictions. On global SFT data collection and aggregation, a few FSB jurisdictions are submitting data to the BIS.

5. Implementation of most FSB recommendations to assess and mitigate systemic risks posed by other non-bank financial entities and activities is ongoing.

The FSB and IOSCO assessed the implementation and effectiveness of their respective recommendations to address liquidity mismatch in open-ended funds (OEFs).

The FSB found that authorities have made meaningful progress in implementing the 2017 FSB Recommendations, but that lessons learnt since then have produced new insights into liquidity management challenges in segments of the OEF sector.

While the assessment suggests that the FSB Recommendations remain broadly appropriate, enhancing clarity and specificity on the policy outcomes the FSB Recommendations seek to achieve would make them more effective from a financial stability perspective.

IOSCO's review of its 2018 Recommendations shows a high degree of implementation of regulatory requirements consistent with the Recommendations' objectives, but some areas may warrant further attention.

In addition to these reforms, the FSB is carrying out further analytical and policy work to enhance the resilience of the NBFI sector, building on the lessons from the March 2020 market turmoil.

To read more: https://www.fsb.org/wp-content/uploads/P180123.pdf

Number 5

Daring to know in times of uncertainty and structural shifts

Klaas Knot, President of the Netherlands Bank and Chair of the Financial Stability Board, at the 11th ILF Conference on the Future of the Financial Sector "The Next Systemic Financial Crisis – Where Might it Come From?": Financial Stability in a Polycrisis World, at the Goethe University's Law and Finance Institute, Frankfurt am Main.

Hello everyone.

This beautiful wood engraving (Note 1) depicts a scene in 1794. You can see four well-dressed men, sitting in a flourishing garden in Jena – a city a few hours east from Frankfurt.

Note 1 "Schiller, Wilhelm and Alexander von Humboldt and Goethe in Jena"(Refers to an external site) (Event date: 1794, image date: 1860). Wood engraving after drawing by Andreas Müller (1831-1901).

The four men are sitting around a table, filled with wine and grapes– and they appear to be engaged in a civilized discussion. The four men on the drawing are the brothers Wilhelm and Alexander von Humboldt,

respectively statesman and explorer, the poet Friedrich von Schiller and, of course, scientist, writer and poet, Johan Wolfgang von Goethe.

The four of them were the intellectual fab four of late 18th century Germany. They strongly believed in the powers of reason – as opposed to royal decrees or religious dogmas. They strongly believed that individuals were to be enlightened – through science, art, and literature. They strongly believed in "sapere aude" – in daring to know.

I was asked to talk about systemic risks today. More precisely, about where the next systemic financial crisis might come from. And truth be told – this is hard to say. We can't predict that with any reliability. One only needs to recall the way that the covid pandemic hit us to know that a crisis can emerge unexpectedly. This is exactly why predicting the next crisis is not what we aim to do at the Financial Stability Board (FSB).

Instead of predicting, our aim is to approach financial stability with a different way of thinking. Financial stability is the capacity of the global financial system to withstand shocks, by containing the risk of disruptions in the financial intermediation process that would be severe enough to adversely impact the real economy.

In short: our work is about enhancing the resilience of the global financial system. So that, when the next crisis materialises, the system as a whole can cope with it.

In order to increase that resilience, we try to know as much as possible about the vulnerabilities in our financial system. And we do this by relying on the powers of reason, logic, cooperation and data. In other words, by following the brothers von Humboldt, Friedrich von Schiller, and Johan Wolfgang von Goethe in sapere aude.

So how do we go about that?

To increase the resilience of the global financial system and to enhance financial stability, we rely on the FSB's financial stability surveillance framework. Let me start by walking you through this framework, and then I will illustrate how we apply it.

The FSB's financial stability framework is based on four guiding principles.

First, we need to identify the vulnerabilities that may threaten global financial stability. I say 'vulnerabilities' instead of 'shocks' or 'risks'. That is intentional.

The pandemic is a shock. The war in Ukraine is a shock. A rapid shift in financial market conditions would be a shock. Shocks are by definition unpredictable – so they don't offer a solid starting point for financial stability policy. Risk – that is the risk of a shock large enough to have a financial stability impact – is similarly very difficult to assess.

Vulnerabilities, on the other hand, can usually be measured, at least to a certain extent. Think for instance about the build-up of imbalances, like a rise in leverage during a credit boom. And so, they do offer a starting point for financial stability policy – policy that is aimed at reducing these vulnerabilities. Through this approach we can mitigate potential systemic disruption, once a shock hits our global, highly interconnected financial system.

And so, in the spirit of Alexander von Humboldt, who measured and mapped large parts of the world, we, in turn, try to map and measure global vulnerabilities – rather than the shocks that may or may not materialise.

Second, once mapped and measured, we monitor these vulnerabilities, taking into account the potential interactions between them. We also deploy a forward-looking perspective, by considering emerging vulnerabilities in addition to current ones. It is better to prevent vulnerabilities from growing in the first place, rather than having to reduce them once they already pose a global threat.

Our third guiding principle is that we recognise the differences among countries. The FSB's membership reflects the diversity of our global financial system, with members from both emerging market and advanced economies. And these differences are reflected in our assessment of vulnerabilities. We fully recognise that some vulnerabilities may be more relevant for emerging market economies, and others for advanced economies, or for different sets of jurisdictions.

For example, the urgency policymakers ascribe to some of the risks relating to crypto-assets and crypto-markets differs across countries. In some economies, the most pressing concern is the potential loss of monetary sovereignty. In other economies, the risks of money laundering and fraud are perceived to be more urgent.

The fourth and final guiding principle, is that the FSB leverages on this diversity of its membership. There lies tremendous strength in that diversity. FSB members not only come from different kinds of economies, but they are also represented by different kinds of authorities: ministries of finance, central banks, and securities and market authorities. Our members also include global standard-setting bodies and international organisations.

Many of those members carry out and publish financial stability assessments. The FSB's vulnerabilities assessment therefore builds on those analyses.

With these four guiding principles, I have given you a brief and mainly theoretical outline of the FSB's financial stability surveillance framework. I hope that this approach, this way of thinking about how to enhance the resilience of the global financial system, provides you with some stimulus for today's discussions.

But what does it look like when we actually apply this framework? To illustrate this, allow me to touch on several of the key FSB priorities that are also on your agenda today.

First, I will focus on the cyclical vulnerabilities that emerge from the current outlook. The combination of rising inflation, tightening financial conditions and the fallout from Russia's invasion of Ukraine has led to a synchronised slowdown in global economic activity.

This is occurring against a backdrop of high levels of debt of households, non-financial corporates and sovereigns. The latter implies that some governments have limited fiscal space to provide additional targeted policy support. And given the increases in inflation, central banks also have less policy space to react to financial stability shocks.

Although this outlook is challenging, so far the global banking system has shown itself to be resilient. Global financial markets have largely coped in an orderly manner, with limited and temporary support when necessary. And systemic financial institutions have shown resilience to market strains – in large part due to the financial reforms, following the 2008 Global Financial Crisis, that were coordinated through the FSB.

However, there is no room for complacency. Financial institutions and market participants have not experienced sharply rising interest rates for a long time. Very low interest rates may have become embedded in business models, making the adjustment to a world of higher rates challenging. Companies and households that have borrowed money will also need to adjust to higher interest payments, and problems may materialise only with a lag.

So, we need to remain vigilant. A deterioration of banks' asset quality may still occur, and other vulnerabilities, like the ones on today's agenda, need to be monitored closely. Some of these vulnerabilities may have been previously prevented from materialising by authorities' COVID-19 support measures. But now these measures are being lifted. So it is important to

address debt overhang issues of non-financial corporates, and to respond to potential issues of underinvestment due to excessive indebtedness or misallocation of resources to unviable companies.

All of these are what I would call cyclical vulnerabilities.

But, more fundamentally, we also need to be wary of vulnerabilities that stem from structural shifts in the global financial system.

So allow me to say a few words on three structural shifts that the FSB is currently focusing on, and the associated vulnerabilities. It is, of course, no coincidence that the topics of today's panels overlap with many of the FSB's priorities.

First – the structural shift in the provision of finance from banks to non-banks.

In our Global Monitoring Report on non-bank financial intermediation, from December 2022, we highlighted that the NBFI sector reached 239 trillion US dollars in 2021. If a number on that scale is hard to put into context, a more telling figure is perhaps that the NBFI sector increased its relative share of total global financial assets to 49% in 2021, compared with 42% in 2008. Almost half of all global financial assets are now being intermediated by non-banks.

While diversifying the sources of credit can make the global economy more resilient, the growth in NBFI has exposed important vulnerabilities in the non-bank sector.

We have seen the problems that these vulnerabilities can cause several times in recent years: for instance, the 'dash for cash' episode during the onset of the pandemic, the strains in commodity markets last year, and more recently the challenges faced by UK pension funds.

Thankfully, these strains have proved temporary, but only after massive official sector interventions were deployed. These examples therefore serve as a warning to remain vigilant on the recurring themes of leverage, including hidden leverage, liquidity mismatches, and data gaps.

The FSB's NBFI work programme and policy proposals aim to address these vulnerabilities. In 2023, we will continue to focus on some key vulnerabilities within the sector. Apart from monitoring systemic risk in NBFI, we will review the effectiveness of our money market funds policy proposals from 2021; revise our recommendations from 2017 on liquidity

mismatches in open-ended funds; and conduct follow-up work on margining practices and hidden leverage in NBFI.

A second structural shift we have witnessed, is the digitalisation of finance. This comes in many shapes and forms, but I will focus on the rapidly developing crypto-asset ecosystem. Crypto-asset markets and activities bear a multitude of risks and vulnerabilities. While the technology behind crypto-assets is often being promoted as game-changing, the vulnerabilities associated with them are in fact quite similar to those we know from traditional finance.

Liquidity mismatches, hidden leverage, and counterparty credit risk are all examples of well-known financial risks that have also materialised in crypto-asset markets in the past year. National regulatory authorities have recognized that these activities are in essence financial activities and have begun regulating them. This is challenging for national authorities, however, because crypto-asset markets are inherently global in reach.

So, in the presence of structural vulnerabilities and in the absence of globally consistent regulation, the FSB is concerned crypto-asset markets may soon pose a challenge to global financial stability.

The FSB therefore concluded that crypto-asset activities and markets must be subject to effective regulation and oversight commensurate to the risks they pose, both at the domestic and international levels.

To this end, the FSB proposed a comprehensive global framework for the effective regulation of crypto-asset activities, including stablecoins, in October last year. This framework embeds the principle of 'same activity, same risk, same regulation'. Finalising these recommendations and monitoring their effective implementation across all jurisdictions will be a priority for the FSB in 2023.

Of course, the FSB does not operate alone. Just like in the traditional financial sector, there is a myriad of functions that the crypto asset ecosystem covers or otherwise touches. So it is key to have solid cooperation between the different standard setting bodies, all with their different mandates.

Third – it is impossible to talk about systemic risk without mentioning one of the most fundamental challenges of our time: climate change.

This third structural shift is not on the agenda today, but the events of the past year have again emphasised the importance of addressing these vulnerabilities. The volatility in energy markets, exposures to

hard-to-predict physical risks and the challenges of the transition to net zero are all examples of vulnerabilities that have an impact on the financial sector.

So addressing the financial risks stemming from climate change is, and will remain, high on the FSB agenda. One way we are working on this, is with our roadmap. With that roadmap, we are coordinating the international efforts to address climate-related financial vulnerabilities. It consists of four key elements: disclosure, data, vulnerability analysis and supervisory and regulatory tools.

One of the main priorities is the reliability and consistency of data, because that is what good risk management starts with. A key priority for this year is the finalisation and implementation of a global climate-related disclosure standard. Other priorities are analysing the use of transition planning and the improvement of our framework for monitoring climate-related vulnerabilities.

Let me wrap up.

NBFI, crypto and climate-related financial risks – these are just three priorities for the FSB and the global financial system I wanted to touch on today.

But for every risk or vulnerability we focus on, be it cyclical or structural, the same principle applies: the FSB diligently maps, measures and monitors all threats to the stability of our global financial system.

We provide a global, cross-border, cross-sectoral and forward-looking perspective on the vulnerabilities we identify. And we do this by drawing on the collective perspective of the broad membership of the FSB.

And this way of working, fearless and in the spirit of “sapere aude”, does not allow me to predict where the next systemic crisis might come from, but it does allow us to enhance the resilience of the global financial system, to whatever may come its way.

In that spirit, the FSB decides where coordinated action is required, monitors the effects of its actions, and assesses where further adjustments are needed. Or, as Goethe said: "Knowing is not enough; we must apply. Willing is not enough; we must do.”

The four men in the wood engraving I talked about at the beginning continue to be an inspiration today. Each with their own merits – and together, as an example of how reason advances humankind.

After Friedrich von Schiller's death, and as an introduction to the correspondence between the two men, Wilhelm von Humboldt wrote an essay on his close association with the famous poet. And in that essay, he stresses the importance Schiller attached to conversation – to how conversation, expressing ideas, exchanging views, ultimately leads to deeper understanding.

To how conversation, you could say, embodies "sapere aude". Or in Schiller's words: "Erkühne dich, weise zu sein".

And this is just the kind of conversation I hope you will have today.

Thank you.

To read more:
https://www.dnb.nl/en/general-news/speech-2023/speech-klaas-knot-daring-to-know-in-times-of-uncertainty-and-structural-shifts/

Number 6

SEC Proposes Rule to Prohibit Conflicts of Interest in Certain Securitizations

The Securities and Exchange Commission proposed a rule to implement Section 27B of the Securities Act of 1933, a provision added by Section 621 of the Dodd-Frank Act.

The rule is intended to prevent the sale of asset-backed securities (ABS) that are tainted by material conflicts of interest.

Specifically, the rule would prohibit securitization participants from engaging in certain transactions that could incentivize a securitization participant to structure an ABS in a way that would put the securitization participant's interests ahead of those of ABS investors.

The Commission originally proposed a rule to implement Section 27B in September 2011.

“I am pleased to support this re-proposed rule as it fulfills Congress’s mandate to address conflicts of interests in the securitization market, which contributed to the 2008 financial crisis,” said SEC Chair Gary Gensler. “This re-proposed rule is designed to help address conflicts of interest arising with market participants taking positions against investors’ interests. Further, as required by Section 621 of the Dodd-Frank Act, the re-proposed rule provides exceptions for risk-mitigating hedging activities, bona fide market making, and certain liquidity commitments. These changes, taken together, would benefit investors and our markets.”

If adopted, new Securities Act Rule 192 would prohibit an underwriter, placement agent, initial purchaser, or sponsor of an ABS, including affiliates or subsidiaries of those entities, from engaging, directly or indirectly, in any transaction that would involve or result in any material conflict of interest between the securitization participant and an investor in such ABS.

Under the proposed rule, such transactions would be “conflicted transactions.” They include, for example, a short sale of the ABS or the purchase of a credit default swap or other credit derivative that entitles the securitization participant to receive payments upon the occurrence of

specified credit events in respect of the ABS. The prohibition on conflicted transactions would commence on the date on which a person has reached, or has taken substantial steps to reach, an agreement that such person will become a securitization participant with respect to an ABS, and it would end one year after the date of the first closing of the sale of the relevant ABS.

The proposed rule would provide certain exceptions for risk-mitigating hedging activities, bona fide market-making activities, and certain commitments by a securitization participant to provide liquidity for the relevant ABS.

The proposed exceptions would focus on distinguishing the characteristics of such activities from speculative trading. The proposed exceptions would also seek to avoid disrupting current liquidity commitment, market-making, and balance sheet management activities.

The public comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

To read more: https://www.sec.gov/news/press-release/2023-17

Number 7

New challenges in a changing world

Christine Lagarde, President of the European Central Bank, at the Deutsche Börse Annual Reception, Eschborn.

Introduction

It is a pleasure to speak with you here in Eschborn, marking the start of the New Year. A new beginning often brings with it new challenges, but it also presents us with plenty of opportunities.

And today I would like to touch on both. Looking at today's global economy, I am reminded of the playwright and poet Bertolt Brecht, who once observed: "Because things are the way they are, things will not stay the way they are."

The global economy finds itself at a crucial turning point. Last year, we began to see the emergence of a "new global map" of economic relationships – one in which geopolitics is increasingly influencing the global economy.

And that in turn has important implications for Europe, which will define the year ahead.

A changing world

This map is defined by three interrelated factors: shocks, supply, and security.

First, with support for an open global trading order on the wane, we are facing new types of shocks to the global economy.

For the past few decades, open trade has supported global growth by allowing countries to "rotate" demand during slumps.

But now it could become a source of volatility. That is because the rise of international free trade – and the stability that comes with it – has historically depended on the backing of a global hegemon.

This was evident during the British Empire in the 19 th century, as it was with American support in the wake of the Cold War.

However, major economies – led by the United States and China – are now increasingly using trade to limit the ambitions of geopolitical rivals.

That could fragment world trade with potentially huge costs. The IMF estimates that severe trade fragmentation may cost global output roughly 7% in the long term – an amount similar to the annual output of Japan and Germany combined.

These geopolitical winds are reshaping the second feature of this new map: supply. We are seeing strategic considerations becoming increasingly important in where suppliers are located.

The US Inflation Reduction Act, for example, is deliberately aimed at "reshoring" production and reducing the country's reliance on strategic imports like batteries.

China is also seeking to reduce its own dependence on the rest of the world. And some surveys suggest that even firms in "non-strategic" sectors are increasingly likely to regionalise their supply chains.

This in turn is leading to the third key feature: the growing importance of security. With the security of supply for critical inputs no longer guaranteed, we are likely to see a new "scramble for resources".

To read more:
https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123_1~2d9786eedf.en.html

Number 8

Statement on Prohibiting Conflicts of Interest in Securitizations

Chair Gary Gensler, Chair of the U.S. Securities and Exchange Commission

Today, the Commission is considering whether to re-propose rules to prohibit a range of market participants that sell or sponsor asset-backed securities (ABS) from taking positions against those very products.

I am pleased to support this re-proposed rule as it fulfills Congress's mandate to address conflicts of interests in the securitization market, which contributed to the 2008 financial crisis.

In the aftermath of the financial crisis, Senator Carl Levin led an investigation into conflicts of interest and other abuses in the securitization markets.

The resulting report (the Levin report) found that a conflict of interest arose when investment banks and other market participants sold securitized assets to investors while simultaneously taking large positions against those assets.

The Levin report said that, in doing so, these market participants from time to time may have put their own interests ahead of investors' interests, and profited at investors' expense.

In response, Congress addressed such conflicts in the securitizations market through Section 621 in the Dodd-Frank Act, an amendment proposed by Senators Levin and Jeff Merkley.

Today, a dozen years after the Commission first proposed rules on this matter, the SEC's work to implement Section 621 remains unfinished. This re-proposed rule seeks to address this unfinished step in Congress's vision for financial reform.

As directed by Congress, today's re-proposed rule would prohibit so-called securitization participants—those who sell or facilitate the sale of an asset-backed security—from engaging in a transaction that would involve or result in a material conflict of interest with investors in that ABS. The prohibition would last for a year after the ABS's first sale.

Further, as required by Section 621 in Dodd-Frank, the re-proposed rule provides exceptions for risk-mitigating hedging activities, bona fide market making, and certain liquidity commitments. Through these congressionally mandated exceptions, the rule would allow these market activities while targeting the conflicts that Congress identified.

Today's re-proposed rule responds to public feedback on the 2011 proposal, as well as developments since then in the ABS market. For example, today's re-proposal clarifies the scope of the prohibited conduct, the exceptions, and the participants subject to the proposal. We would benefit greatly from public comment to help us further evaluate these matters.

This re-proposed rule is designed to help address conflicts of interest arising with market participants taking positions against investors' interests. That would benefit investors and our markets.

To read more:
https://www.sec.gov/news/statement/gensler-statement-prohibiting-conflicts-interest-securitizations-012523

Number 9

Ransomware-as-a-service (RaaS) - Cybercriminals stung as HIVE infrastructure shut down

Europol supported German, Dutch and US authorities to shut down the servers and provide decryption tools to victims

Europol supported the German, Dutch and US authorities in taking down the infrastructure of the prolific HIVE ransomware. This international operation involved authorities from 13 countries* in total. Law enforcement identified the decryption keys and shared them with many of the victims, helping them regain access to their data without paying the cybercriminals.

* Canada – Royal Canadian Mounted Police (RCMP) & Peel Regional Police
France: National Police (Police Nationale)
Germany: Federal Criminal Police Office (Bundeskriminalamt) and Police Headquarters Reutlingen – CID Esslingen (Polizei BW)
Ireland: National Police (An Garda Síochána)
Lithuania: Criminal Police Bureau (Kriminalinės Policijos Biuras)
Netherlands – National Police (Politie)
Norway: National Police (Politiet)
Portugal: Judicial Police (Polícia Judiciária)
Romania: Romanian Police (Poliţia Română – DCCO)
Spain: Spanish Police (Policía Nacional)
Sweden: Swedish Police (Polisen)
United Kingdom – National Crime Agency
USA – United States Secret Service, Federal Bureau of Investigations

In the last year, HIVE ransomware has been identified as a major threat as it has been used to compromise and encrypt the data and computer systems of large IT and oil multinationals in the EU and the USA. Since June 2021, over 1 500 companies from over 80 countries worldwide have fallen victim to HIVE associates and lost almost EUR 100 million in ransom payments.

Affiliates executed the cyberattacks, but the HIVE ransomware was created, maintained and updated by developers. Affiliates used the double extortion model of 'ransomware-as-a-service'; first, they copied data and then encrypted the files.

Then, they asked for a ransom to both decrypt the files and to not publish the stolen data on the Hive Leak Site. When the victims paid, the ransom

was then split between affiliates (who received 80 %) and developers (who received 20 %).

Other dangerous ransomware groups have also used this so-called ransomware-as-a-service (RaaS) model to perpetrate high-level attacks in the last few years. This has included asking for millions of euros in ransoms to decrypt affected systems, often in companies maintaining critical infrastructures.

Since June 2021, criminals have used HIVE ransomware to target a wide range of businesses and critical infrastructure sectors, including government facilities, telecommunication companies, manufacturing, information technology, and healthcare and public health.

In one major attack, HIVE affiliates targeted a hospital, which led to severe repercussions about how the hospital could deal with the COVID-19 pandemic. Due to the attack, this hospital had to resort to analogue methods to treat existing patients, and was unable to accept new ones.

The affiliates attacked companies in different ways. Some HIVE actors gained access to victim's networks by using single factor logins via Remote Desktop Protocol, virtual private networks, and other remote network connection protocols.

In other cases, HIVE actors bypassed multifactor authentication and gained access by exploiting vulnerabilities. This enabled malicious cybercriminals to log in without a prompt for the user's second authentication factor by changing the case of the username.

Some HIVE actors also gained initial access to victim's networks by distributing phishing emails with malicious attachments and by exploiting the vulnerabilities of the operating systems of the attacked devices.

About EUR 120 million saved thanks to mitigation efforts
Europol streamlined victim mitigation efforts with other EU countries, which prevented private companies from falling victim to HIVE ransomware.

Law enforcement provided the decryption key to companies which had been compromised in order to help them decrypt their data without paying the ransom. This effort has prevented the payment of more than USD 130 million or the equivalent of about EUR 120 million of ransom payments.

Europol facilitated the information exchange, supported the coordination of the operation and funded operational meetings in Portugal and the

Netherlands. Europol also provided analytical support linking available data to various criminal cases within and outside the EU, and supported the investigation through cryptocurrency, malware, decryption and forensic analysis.

On the action days, Europol deployed four experts to help coordinate the activities on the ground.

Europol supported the law enforcement authorities involved by coordinating the cryptocurrency and malware analysis, cross-checking operational information against Europol's databases, and further operational analysis and forensic support.

Analysis of this data and other related cases is expected to trigger further investigative activities.

The Joint Cybercrime Action Taskforce (J-CAT) at Europol also supported the operation.

This standing operational team consists of cybercrime liaison officers from different countries who work on high-profile cybercrime investigations.

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime, and other serious and organized crime forms.

Europol also works with many non-EU partner states and international organisations.

From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) tackles the most important threats posed by organised and serious international crime affecting the EU. EMPACT strengthens intelligence, strategic and operational cooperation between national authorities, EU institutions and bodies, and international partners. EMPACT runs in four-year cycles focusing on common EU crime priorities.

To read more:
https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down#empact

Number 10

U.S. Department of Justice Disrupts Hive Ransomware Variant

FBI Covertly Infiltrated Hive Network, Thwarting Over $130 Million in Ransom Demands

The Justice Department announced its months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.

Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay $130 million in ransom demanded.

Since infiltrating Hive's network in July 2022, the FBI has provided over 300 decryption keys to Hive victims who were under attack. In addition, the FBI distributed over 1,000 additional decryption keys to previous Hive victims.

Finally, the department announced today that, in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit, it has seized control of the servers and websites that Hive uses to communicate with its members, disrupting Hive's ability to attack and extort victims.

"Last night, the Justice Department dismantled an international ransomware network responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world," said Attorney General Merrick B. Garland. "Cybercrime is a constantly evolving threat. But as I have said before, the Justice Department will spare no resource to identify and bring to justice, anyone, anywhere, who targets the United States with a ransomware attack. We will continue to work both to prevent these attacks and to provide support to victims who have been targeted. And together with our international partners, we will continue to disrupt the criminal networks that deploy these attacks."

"The Department of Justice's disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators,"

said Deputy Attorney General Lisa O. Monaco. “In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than $130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat.”

“The coordinated disruption of Hive’s computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard,” said FBI Director Christopher Wray. “The FBI will continue to leverage our intelligence and law enforcement tools, global presence, and partnerships to counter cybercriminals who target American business and organizations."

“Our efforts in this case saved victims over a hundred million dollars in ransom payments and likely more in remediation costs,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division. “This action demonstrates the Department of Justice’s commitment to protecting our communities from malicious hackers and to ensuring that victims of crime are made whole. Moreover, we will continue our investigation and pursue the actors behind Hive until they are brought to justice.”

“Cybercriminals utilize sophisticated technologies to prey upon innocent victims worldwide,” said U.S. Attorney Roger Handberg for the Middle District of Florida. “Thanks to the exceptional investigative work and coordination by our domestic and international law enforcement partners, further extortion by HIVE has been thwarted, critical business operations can resume without interruption, and millions of dollars in ransom payments were averted.”

Since June 2021, the Hive ransomware group has targeted more than 1,500 victims around the world and received over $100 million in ransom payments.

Hive ransomware attacks have caused major disruptions in victim daily operations around the world and affected responses to the COVID-19 pandemic. In one case, a hospital attacked by Hive ransomware had to resort to analog methods to treat existing patients and was unable to accept new patients immediately following the attack.

Hive used a ransomware-as-a-service (RaaS) model featuring administrators, sometimes called developers, and affiliates.

RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.

Hive actors employed a double-extortion model of attack. Before encrypting the victim system, the affiliate would exfiltrate or steal sensitive data. The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data. Hive actors frequently targeted the most sensitive data in a victim's system to increase the pressure to pay. After a victim pays, affiliates and administrators split the ransom 80/20. Hive published the data of victims who do not pay on the Hive Leak Site.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Hive affiliates have gained initial access to victim networks through a number of methods, including: single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols; exploiting FortiToken vulnerabilities; and sending phishing emails with malicious attachments.

For more information about the malware, including technical information for organizations about how to mitigate its effects, is available from CISA, visit https://www.cisa.gov/uscert/ncas/alerts/aa22-321a

Victims of Hive ransomware should contact their local FBI field office for further information.

The FBI Tampa Field Office, Orlando Resident Agency is investigating the case.

Trial Attorneys Christen Gallagher and Alison Zitron of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Chauncey Bratt for the Middle District of Florida are prosecuting the case.

The Justice Department also recognizes the critical cooperation of the German Reutlingen Police Headquarters-CID Esslingen, the German Federal Criminal Police, Europol, and the Netherlands Politie, and significant assistance was provided by the U.S. Secret Service, U.S. Attorney's Office for the Eastern District of Virginia, and U.S. Attorney's Office for the Central District of California. The Justice Department's Office of International Affairs and the Cyber Operations International Liaison also

provided significant assistance. Additionally, the following foreign law enforcement authorities provided substantial assistance and support: the Canadian Peel Regional Police and Royal Canadian Mounted Police, French Direction Centrale de la Police Judiciaire, Lithuanian Criminal Police Bureau, Norwegian National Criminal Investigation Service in collaboration with the Oslo Police District, Portuguese Polícia Judiciária, Romanian Directorate of Countering Organized Crime, Spanish Policia Nacional, Swedish Police Authority, and the United Kingdom's National Crime Agency.

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 individual or entity;

- should not be relied on in the 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 regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

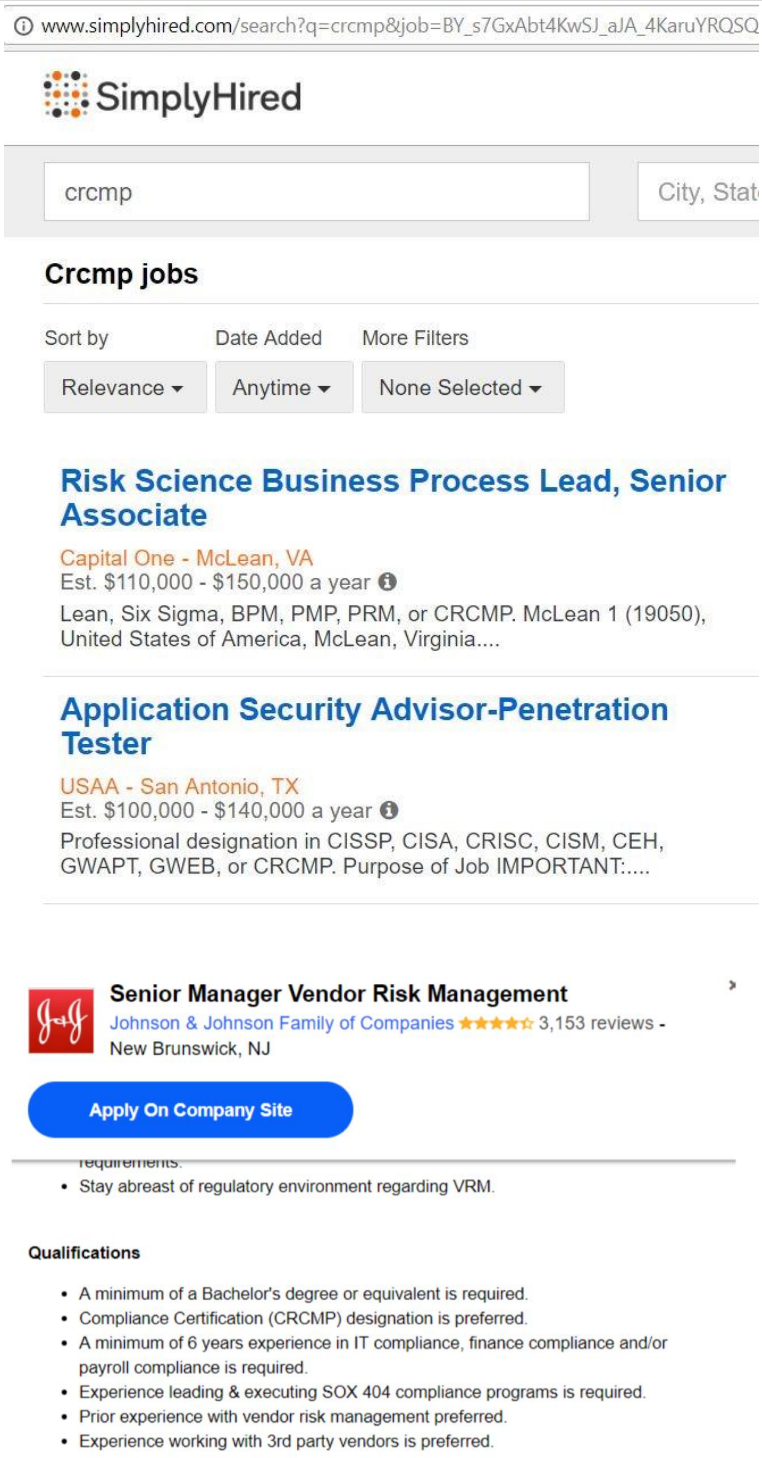
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

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