Monday, October 19, 2020

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,

I have just read the *Internet Organized Crime Threat Assessment (IOCTA) of 2020*. This is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime.

It provides a unique law enforcement focused assessment of emerging challenges and key developments in the area of cybercrime.

According to the assessment, continuing innovative developments of recent years, criminals are *offering full digital user profiles* in order to bypass advanced fraud prevention tools.

In keeping up with e-commerce merchants increasingly employing analytics checking a user's identity against device fingerprints and several other metrics, criminals have moved to *obtaining and selling* these digital profiles to commit fraud.

Taken from machines compromised in a botnet, they are used in order to make purchases using the compromised computer pretending to be a returning customer, using the same browser settings and victim's card credentials.

After the fraud, many victims erase the evidence themselves, following Windows security guidance to restore to the last known configuration after having been compromised by the botnet, effectively removing all traces of the intrusion.

This use of botnets to bypass sophisticated fraud prevention tools reflects a recurrent theme in the fight against cybercrime – as security measures are

heightened, criminals come up with novel ways to continue their illicit activities.

There has been an increase in the provision of digital and cybercrime elements on the *Darkweb*. Personal data, access to compromised systems, as well as services catering malware, ransomware, and DDoS attacks, are all elements prevalent for the facilitation of cybercrime.

Document and proof of identity services have also increased on the Darkweb. Perpetrators generally use identity and document services to support citizenship claims and other applications, obtaining lines of credit to set up a business, open untraceable bank accounts, proof of residence, to commit insurance fraud, purchase illicit items and other uses.

There has been a shift in the offering of *legitimate-looking counterfeit passports* to "legal or registered" passports, which can pass several authentication tests, with criminals offering registered passport services.

Trend Micro Inc. has explained that the increase of global immigrants and the increasing adoption of e-passports is a likely driver behind this trend.

Additionally, some Darkweb sites also promote money laundering and instructions for users on how to use cryptocurrencies for money laundering. Users can find drug listings in massive volume on the Darkweb; however, these do not necessarily reach priority-levels in terms of impact.

More impactful, dangerous drugs, such as fentanyl, opioids and heroin are still significantly present on the Darkweb, although listings are smaller in number.

Europol has observed an increasing trend of top organised crime groups having a presence on the Darkweb dealing drugs, which is likely due to an effort to expand their distribution mechanisms.

As noted in IOCTA 2019, drug dealers may also be running multiple monikers on the Darkweb which makes it difficult to prioritise within the drug topic.

Additionally, the COVID-19 pandemic crisis seemed to have the most effect on the supply chains regarding drug trade compared to other crime. This has now stabilised and the situation has returned to normal, with an anticipated growth on the horizon.

Finally, the distribution of firearms has become significantly more fragmented. After the takedown of the Berlusconi marketplace by Italian

law enforcement, which used to be the go-to place for firearms on the Darkweb, firearms have emerged on different marketplaces.

Firearms are also available on OpenBazaar, although the scale of supply is unconfirmed. Some shops are also selling firearms from the United States.

The ability for individuals to purchase firearms on the Darkweb has become increasingly difficult, due to recent law enforcement successes in catching individuals purchasing firearms illegally.

The diverse products and services vary in their level of impact and their ability to facilitate more serious forms of crime.

The supply of these goods on the Darkweb poses a significant threat in the EU. Furthermore, the geographic nature of the threat is also diversifying.

The Hydra market – the largest darknet marketplace serving Russia and neighbouring countries – has recently advertised an impending publication of a new, secure encrypted market platform, which they aim to open to the English-speaking community.

Such a development would arguably make Darkweb investigations more difficult for law enforcement in the future and poses a significant threat to the EU.

Read more at number 6 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 7)

Mortgage market regulation and access to mortgage credit

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at "Opportunities and Challenges for Homeownership," a Virtual Roundtable Discussion, Bozeman.

Number 2 (Page 11)

What got us here will not get us there - how the EU and Germany are preparing finance for a new age

Dr Sabine Mauderer, Member of the Executive Board of the Deutsche Bundesbank, at the virtual conference of CFA Institute and CFA Society Germany

Number 3 (Page 15)

When the unconventional becomes conventional

Claudio Borio, Head of the BIS Monetary and Economic Department
The ECB and Its Watchers XXI, Frankfurt

Number 4 (Page 18)

Covid-19 - A digitalisation boost and the supervisory response

Frank Elderson, Executive Director of Supervision of the Netherlands Bank, at the SSM Roundtable, Berlin.

Number 5 (Page 23)

Homeland Threat Assessment, October 2020

Homeland Security

Number 6 (Page 26)

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020

EUROPOL

Number 7 (Page 32)

A solution to every puzzle

John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at the 2020 US Treasury Market Conference

Number 8 (Page 36)

Speech at the Congress of the Association of Banks of Russia

Elvira Nabiullina, Governor of the Bank of Russia, at the Congress of the Association of Banks of Russia, Moscow.

Number 9 (Page 44)

Cloud Security: The way forward?

National Cyber Security Centre

Number 10 (Page 45)

NIST Crowdsourcing Challenge to De-Identify Public Safety Data Sets

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

Number 1

Mortgage market regulation and access to mortgage credit

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at "Opportunities and Challenges for Homeownership," a Virtual Roundtable Discussion, Bozeman.

Good afternoon, everyone. Thank you to Montana State University (MSU) for hosting today's event and for that very kind introduction. It is wonderful to see the success of your Community Banking Program here at MSU and your commitment to investing in the education of future generations of community bankers.

Throughout the response to the pandemic, community bankers have continued to serve as the primary source of credit to small businesses and have continued to provide economic and financial support to communities across our nation.

Young people, like all of you engaged in this program, will very likely become the future leaders of these institutions, which are critical to their communities and to our economy and financial system.

One of the most significant challenges facing community bankers today is navigating the complex regulatory framework. One area that has become more complicated is a line of business that has traditionally been the foundation for community banking, home mortgage lending.

Community bank leaders consistently tell me that significant regulatory burden related to making home mortgages has been a major reason they have scaled back their mortgage lending activities or exited the market altogether.

Along with tightened lending standards, this trend has made it harder for middle- and lower-income borrowers to obtain mortgage credit since the global financial crisis.

Fortunately, work is under way to relieve that burden, and I will highlight one effort in particular. But before I do, let me provide some context by

reviewing the current state of the economy and its effect on homeowners and would-be homeowners.

The COVID-19 Pandemic and Homeownership in the U.S.

The COVID-19 pandemic is having a profound effect on individuals and families across the U.S. and throughout the world. While a strong recovery has begun, it is clear that there is still a way to go before we are back to the robust economy we experienced at the beginning of the year.

These challenges are affecting homeowners and the lenders that provide credit to support them. Many homeowners who have lost a job or have had their income affected by economic conditions have been able to work with their lenders, but such help may not be a long-term solution for many borrowers.

Fortunately, the housing market as a whole is a bright spot for the economy. Higher home prices are improving the balance sheets of many households, even those that may face income and employment challenges, and new construction activity is generating new job opportunities.

While affordability remains an important consideration, it is encouraging that housing has performed well in response to low interest rates.

Mortgage Regulations and Access to Mortgage Credit

However, even during this period of strong performance in the housing market, access to affordable mortgage credit remains a barrier to homeownership for some borrowers, due in part to regulatory burden.

Since the last financial crisis more than a decade ago, there have been a number of new mortgage regulations that added requirements for both borrowers and lenders.

While many of these requirements have contributed to a safer and more consumer-friendly mortgage market, they have also introduced significant paperwork and delays that can present roadblocks for many borrowers.

These new rules have also made it more difficult and costly for small banks to originate mortgage loans, leading many community banks to scale back on home lending activity or abandon it altogether.

Homeownership is as important to communities as it is to individuals, and access to credit for rural and low-to-moderate income communities often depends on community banks. In many communities, especially rural

communities, if the local bank has been forced out of mortgage lending due to burdensome regulation, it means little or no access to mortgage credit, preventing buyers from financing home purchases and homeowners from selling their homes.

Many leaders of small community banks have told me that the compliance costs for originating smaller mortgages are prohibitive, and that the staffing and training required to meet the strict requirements are extraordinary in relation to the limited number of mortgages they originate.

As one state banking commissioner said to me recently, "It doesn't make a lot of sense that you can make an $80,000 truck loan on two sides of a sheet of paper, but that many, many pages of paperwork are required to make a $40,000 loan on a mobile home or trailer."

In fact, I have been told by community bankers that they are sometimes compelled to make loans for lower-priced home purchases that are backed by other collateral, such as a car or equipment, because of the excessive burden of complying with the many residential home mortgage regulations and time frames for such small transactions.

As a result, these consumers may not have the benefit of the important consumer protections that having a home mortgage loan provides.

Reducing mortgage compliance burden would allow community banks to better meet the critical need for home lending in their communities.

Because of their local knowledge and strong customer relationships, community banks are often more willing to work with borrowers to get through difficult times.

Taking steps to simplify and lower this regulatory burden for small community banks and their customers would help to ensure that homeowners can stay in their homes during times of stress, like the one we are facing currently due to COVID-19.

One Area to Consider in Easing Burden

The TILA-RESPA Integrated Disclosure, or TRID, is one of the real estate regulatory requirements that smaller banks cite most frequently as creating a heavy burden.

Commissioner Melanie Hall and the Montana Independent Bankers have been particularly helpful in highlighting the importance of this issue.

Therefore, I am very pleased that the Independent Community Bankers of America is engaged in ongoing conversations and activities to address the more burdensome aspects of this requirement on community banks while importantly retaining key consumer protections.

Efforts like these that aim to reduce the compliance burden for critically important services will enable many community banks to return to doing what they do best: meeting the needs of their communities.

Again, thank you for inviting me to join you today, and I look forward to engaging on this important topic.

Number 2

What got us here will not get us there - how the EU and Germany are preparing finance for a new age

Dr Sabine Mauderer, Member of the Executive Board of the Deutsche Bundesbank, at the virtual conference of CFA Institute and CFA Society Germany

1 Introduction

Today, we are looking at the crucial question of how the EU and Germany are preparing finance for a new age.

As a central banker, let me start with monetary policy and a clear assessment.

2 The role of the Eurosystem for capital markets during the pandemic

The Eurosystem's monetary policy has helped prevent an impairment of the financial system that would have aggravated the economic crisis.

At the beginning of the COVID-19 crisis, the economic outlook deteriorated at an unprecedented speed and financial conditions tightened.

Above all, there was a danger that the financial sector might become impaired and that this could make the severe slump in the real economy even worse.

As the financial crisis taught us, such a negative feedback loop could seriously impede price stability in the medium term.

In order to avert this, monetary policy action was needed.

Providing banks with an ample supply of liquidity, coupled with low interest rates, helps to ensure that the economic crisis is not further aggravated by the financial system.

And, indeed, the ECB Governing Council adopted a broad set of measures, including asset purchases, long-term central bank loans and collateral framework adjustments.

In particular, the pandemic emergency purchase programme (PEPP) helped reduce systemic stress in financial markets.

After the announcement of the PEPP, financial conditions for companies, households and governments clearly improved in the euro area.

Moreover, during spring, it became clearer that the crisis would dampen future consumer prices.

Therefore, further monetary policy action was warranted in June, given our mandate to ensure price stability.

3 Outlook: The price stability mandate as the yardstick for the Eurosystem's role

Our mandate is where my second message comes in. Looking ahead, fulfilling our price stability mandate with adequate measures should continue to be the yardstick for the Eurosystem's role in capital markets.

The Governing Council has to keep checking whether its measures are suitable and well-designed in order to choose the right instruments and to design programmes prudently.

Any assessment of a monetary policy measure has to compare the degree to which this measure contributes to achieving the monetary policy objective on the one side, with possible unintended side-effects on the other.

Moreover, it requires a judgement as to whether other policy measures are available that offer a better balance between intended and unintended effects.

Clearly, bond purchases are a legitimate and effective monetary policy instrument.

But large-scale government bond purchases come with risks and potential side-effects, especially the risk of blurring the lines between monetary and fiscal policy.

This is particularly problematic in the context of a monetary union. Therefore, government bond purchases under the special terms of the monetary union should be an emergency tool.

Moreover, crisis-related monetary policy measures must be limited, both in duration and volume. Let's not forget that the letter "E" in PEPP stands for "emergency": the PEPP must be scaled back when the emergency is over.

Similarly, crisis support for enterprises from fiscal policy must also be temporary.

4 The pandemic as a push for companies to diversify their funding

At the same time, the prospect of less support should be a reminder for firms to check their funding options, not just in Germany but further afield, too. And this brings me to my final message today.

The pandemic should be a strong push for German companies to diversify their funding. The German capital market's potential has not been fully utilized yet.

There's no denying that many German companies have done a pretty good job of withstanding the financial fallout of the pandemic, on the back of strong individual balance sheets.

Yet the crisis revealed that there can be situations when liquidity is precious and scarce.

Some companies were heavily reliant on bank funding, but in the absence of monetary policy and fiscal support, banking lending would have been undermined by the pandemic shock as well.

So having more diversified funding options, including the ability to tap capital markets, would have made sense.

At the same time, some Eurosystem central banks, including the Bundesbank, found that our corporate sector purchase programme (CSPP) was unable to support companies in all euro area countries in the same way.

Why was that? Because some financial market segments are still relatively underdeveloped on a national level. The German commercial paper market is a case in point.

But it was not just the weaknesses in terms of debt funding options that were laid bare.

The pandemic also supported the notion that research and innovation are most advanced where equity and venture capital, or hybrid forms of financing are readily available.

So these funding options - ideally of a cross-border variety - should be top of the capital market agenda, in Germany and elsewhere in the euro area.

5 Conclusion

Ladies and gentlemen, allow me to stop here and conclude.

First, during the pandemic, central bank support helped prevent a negative feedback loop between the financial system and the real economy.

But, secondly, emergency measures need to be scaled back once the emergency is over.

And third, the pandemic is teaching us that in order to be future-proof, economies have to be fast and innovative in adapting to a new environment. Against this background, the pandemic crisis needs to be a strong push to make European capital markets true drivers of real economic innovation. And German companies need to put their funding side on a broader basis.

Many thanks for your attention.

Number 3

When the unconventional becomes conventional

Claudio Borio, Head of the BIS Monetary and Economic Department
The ECB and Its Watchers XXI, Frankfurt

Abstract

The tools central banks use for crisis times are becoming increasingly indistinguishable from those they employ for normal times; the unconventional is becoming conventional.

The tools in question have proved more effective than generally expected in influencing financial conditions, but appear to exhibit diminishing effectiveness and have long-term side effects.

Partly as a result, the wide-ranging and forceful emergency measures taken to address the Covid-19 crisis have further reduced the policy room for manoeuvre.

An economy with small safety margins is exposed and vulnerable.

As soon as conditions allow, the priority will be to rebuild policy buffers, not just in monetary policy, but also in prudential and fiscal policies.

Monetary policy will face a particularly tough twin challenge: economic, owing to the limited responsiveness of inflation to economic slack; and intellectual, given the popularity of the notion of the natural interest rate – a real rate fully independent of monetary policy.

That notion puts central banks in a straightjacket.

Thank you for inviting me to this event. I am glad to be speaking here again. This session is about the ECB's toolkit for normal and crisis times.

I hope you will excuse me if I don't speak about the ECB specifically, but about central banking in general.

Of course, some of the points I'll be making are relevant to the ECB too. After briefly retracing the extraordinary monetary journey since the Great Financial Crisis (GFC), I would like to focus on three issues: the lessons, the caveats and the challenges.

The bottom line is that there are tough policy challenges ahead, and the answers remain elusive.

The journey

So, let me recap the monetary journey.

It is a sign of the extraordinary times we live in that the central bank tools for normal and crisis times are increasingly hard to distinguish. In the "old days", the picture was quite simple.

In normal times, central banks would steer the market overnight rate within a positive range.

Liquidity management operations would work in the background. They would be designed purely to steer that rate, and carried no signal about the monetary policy stance.

In crisis times, central banks would actively use their balance sheet in order to stabilise financial markets and institutions, typically through emergency liquidity assistance to financial institutions, essentially banks.

One possible exception to this neat distinction, at least for some of them, most notably those in emerging market economies (EMEs), was FX intervention. This is a type of balance sheet policy in all but name.

Then came the GFC, which upended this simple world. In its wake, central banks started to actively deploy their balance sheet in order to spur aggregate demand, given the proximity of the effective lower bound.

The balance sheet became a key tool to set the monetary policy stance. Hence the large-scale purchases of public sector and private sector securities and, in the euro area, public sector securities of different degrees of credit risk as well as special subsidised lending schemes for banks.

In addition, central banks began to rely heavily on forward guidance, extending way into the future, as a quasi-commitment device.

And some of them also pushed interest rates into negative territory.

This was something historically unprecedented and would simply have been unthinkable until then.

The cross-country differences that do exist do not invalidate this general picture.

The response to the Covid-19 crisis is yet another step along that path.

Central banks have done more, in terms of both scope and amounts; hence the more direct support for firms of lower credit quality. And more central banks have done so; hence, for instance, the unprecedented large-scale purchases of government securities in EMEs.

In the process, central banks have crossed a number of red lines, and they have done so with their eyes wide open: emergency times call for emergency measures.

We have described and analysed this in detail in a chapter of our latest Annual Economic Report.

Looking forward, if the post-GFC experience is anything to go by, it is not inconceivable that some of these tools will survive and become part of the normal toolkit.

To read more: https://www.bis.org/speeches/sp200930.pdf

Number 4

Covid-19 - A digitalisation boost and the supervisory response

Frank Elderson, Executive Director of Supervision of the Netherlands Bank, at the SSM Roundtable, Berlin.

As the COVID-19 pandemic unfolded back in March of this year, suddenly hundreds of thousands of financial sector workers were working from home. From board members to secretaries, our homes became our new offices, Skype became our new meeting room.

That was a major shock but we adapted quickly. IT systems that once took ages to implement were rolled out in a matter of weeks. Network capacity was stepped up in record time.

Also, the trend from cash to digital payments accelerated. Just before the lockdown in mid-March, the Dutch used cash for 3 out of 10 retail payments.

Now, they use it for only 2 out of 10 retail payments. That's a huge drop in cash usage in only a few months' time. In addition, we have seen a large increase in online payments.

What happened back in March could perhaps best be compared with a swimming pool. A year ago, we were merely dipping our toes. COVID-19 pushed us in, and now we are swimming!

What is now very clear, is that COVID-19 has accelerated digitalization. Many of these developments are welcome. First and foremost, thanks to our digitalization jump, the financial system largely continued to function as normal.

As the world economy went into lockdown, the financial system remained open. This is a remarkable feat.

One that bears witness to the operational resilience of the financial sector and to the power and opportunities that digitalization has brought us.

Another upside is that customers are getting more used to doing things digitally. This opens up opportunities for banks to introduce new products and to reduce costs.

On the risk side, it is notable there were no major operational incidents during the pandemic. At the same time, operational and especially cyber risks have clearly increased.

Since COVID-19 we have seen a spike in cyber threats, like ransomware attacks and phishing. And both the risk and possible impact of operational incidents caused by people, failed processes and systems has increased as a result of greater reliance on virtual working arrangements.

For example, we have seen that several third party providers suffered ransomware attacks that could have severely affected the financial sector.

The big question financial institutions and supervisors need to keep asking themselves, especially in the current environment: is our operational resilience keeping up with the faster pace of digital developments?

When it comes to Fintech, I think COVID-19 has also accelerated existing trends there too. The future development of Fintech is a function of technological innovation and changing consumer preferences.

COVID-19 did not immediately bring new technology, but it may have moved consumer preferences more towards digital. People kept contact with each other via Zoom and Face Time and Skype.

School children all over the world followed online lessons. Online retail went through the roof. From there, it may only be a small step to paying with Whatsapp, or getting a mortgage from Quicken Loans.

So COVID-19 may have influenced digitalization in many different ways. If there is anything the COVID-19 pandemic has taught us here, it is that adoption of new technology is non-linear.

When technology is already available, sometimes it takes only one event to cause a sudden and decisive shift in consumer preferences.

This adds all the more urgency to the big questions already on the table before the pandemic.

How will Fintech impact the business model of traditional banks?

What role will bigtech firms play?

When the lines between banks and technology firms become more and more blurred, who is responsible for security and financial stability?

Do we understand the algorithms that are being applied increasingly in banking?

How do new technologies influence cyber and financial crime?

Are supervisors sufficiently equipped, in terms of knowledge and staff, to keep up with developments?

Where are the holes and obstacles in regulation?

What does it mean for the level playing field when regulated and unregulated entities compete on the same markets?

How can supervisors themselves use the new technologies to improve supervisory practices?

And last but not least, there are social issues involved in digitalization. Not everyone can keep pace with the current tempo of digitization. Digital exclusion of vulnerable groups of consumers, like the elderly or people on a low income, is a serious issue nowadays.

This is only a subset of a vast area of questions that are relevant to the stability of the financial system. But I have total confidence this panel of eminent experts will be able to answer these questions shortly.

This brings me to the last issue I would like to raise. How should supervisors respond to these changes?

There used to be a time when financial supervision was viewed as basically reactive. The idea was that, by nature, supervisors are always at least one step behind the market, and that we should aim to keep the gap as narrow as possible.

I think supervisors that still adhere to that view are missing the demands of the new times. If ever, in the current landscape, with fast but fundamentally uncertain changes, supervisors should be forward looking and adaptive.

By forward looking I do not mean supervisors like me can predict the future.

We can't. And we are probably worse at it than the industry. But we should stay on top of developments, think in terms of scenarios, and broaden the

dialogue from the financial sector to important tech and infrastructure players.

And I think this also a good approach when it comes to the development of new regulation, notably the European Commission proposals on the regulation of the use of cloud services by the financial sector, and it digital strategy.

And when I say supervisors should be adaptive, what I mean is to acknowledge the fact that existing regulation was often drafted with a different world in mind, that this regulation cannot always be literally applied to the new digital world.

Adaptive then means to act from a set of core principles.

To apply them in a way that fits the new environment and leaves space for innovation.

While continuing to protect customers and financial stability. To give you an example, two months ago we published a discussion paper called 'General principles for the use of Artificial Intelligence in the financial sector'.

To sum it up in one sentence: firms should pay due attention to the soundness, accountability, fairness, ethics, skills and transparency aspects of the applications they develop.

We are using this discussion paper, and the comments received, to engage in a dialogue with the Dutch financial sector about the use of AI.

Finally, new technology also creates opportunities for supervisors to improve their own effectiveness. In 2018 De Nederlandsche Bank set up a dedicated Supervision Innovation Department to coordinate and accelerate the implementation of its digital strategy.

The strategy's purpose is to adopt a more data-driven approach and deploy technology to support the supervisory process. The ultimate goal is to transform DNB into a 'smart supervisor'.

Also, when it comes to supervision, Covid-19 has increased the awareness of the potential of digitalization.

Digital processes are not susceptible to the impact of reduced staff availability during a lockdown.

It also increased the broad mindset that digitalization is the new normal and boosted acceptance of working with new digital tools throughout the entire workforce.

So to sum up, COVID-19 has stepped up the pace of digital developments. This has given more urgency to the policy questions already on the table. It requires supervisors to be forward looking and adaptive, and to keep up with developments to improve their own supervisory practice.

I'll stop here and I look forward to hearing your insights during the discussion.

Number 5

Homeland Threat Assessment, October 2020

Homeland Security

The Department of Homeland Security (DHS) is the first and last line of defense against the many threats facing our country.

Our ability to mitigate these threats is predicated on our ability to understand them and to inform the American people.

The DHS Homeland Threat Assessment (HTA) identifies the primary threats facing the United States of America at and inside our borders.

This Assessment draws upon all sources of information and expertise available to the Department, including from intelligence, law enforcement, and our operational components.

The purpose of the HTA is to provide the American people with an overview of the information collected and analyzed by DHS employees around the world and provided to the Secretary of Homeland Security.

The HTA is primarily informed by intelligence analysis prepared by the DHS Office of Intelligence and Analysis (I&A) and by the Component intelligence offices, which identified the leading security threats to the Homeland based on a review of all-source intelligence information and analysis.

Given the array of potential issues, I&A's scoped its analysis to focus on key threats covered by the intelligence elements of the Department, which expert analysts considered most likely and with the potential to significantly affect U.S. security.

The HTA was also informed by the expertise and insights of the Department's Operational Components, which assess and respond to threats on a daily basis, as well as the informed views of the DHS Office of Strategy, Policy, and Plans (PLCY), which leads threat identification and prevention activities.

This inaugural HTA presents a holistic look from across the Department and provides the American people with the most complete, transparent, and candid look at the threats facing our Homeland.

It breaks down the major threats to the Homeland in the following sections:

1. The Cyber Threat to the Homeland
2. Foreign Influence Activity in the Homeland
3. Threats to U.S. Economic Security
4. The Terrorist Threat to the Homeland
5. Transnational Criminal Organization Threats to National Security
6. Illegal Immigration to the United States
7. Natural Disasters

OPPORTUNITY FOR CYBER ACTORS TO EXPLOIT COVID-19

Both cybercriminals and nation-state cyber actors—motivated by profit, espionage, or disruption—will exploit the COVID-19 pandemic by targeting the U.S. healthcare and public health sector; government response entities, such as the U.S. Department of Health and Human Services and the Federal Emergency Management Agency; and the broader emergency services sector.

- Cybercriminals most likely will deploy ransomware for financial gain, whereas nation-state cyber actors might seek to capture insights into U.S. response plans and scientific information related to testing, therapeutics, and vaccine development.
- We expect that cybercriminals and nation-state cyber actors will target victims in the United States with COVID-19-themed spear-phishing e-mails, which we already have observed overseas. These e-mails appear to claim to be from official government sources, including the U.S. Centers for Disease Control and Prevention and the U.S. Department of State.

FOREIGN INFLUENCE DEFINITIONS:

Foreign Influence. Any covert, fraudulent, deceptive, or unlawful activity of foreign governments—or persons acting on their behalf—undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting U.S. democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives.

- Covert Influence: Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action.
- Overt Influence: Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda.
- Disinformation: A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests.
- Misinformation: Foreign use of false or misleading information. Misinformation is broader than disinformation because it targets a wide audience rather than a specific group.

To read more:
https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

Number 6

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020

The IOCTA is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime.

It provides a unique law enforcement focused assessment of emerging challenges and key developments in the area of cybercrime.

We are grateful for the many contributions from our colleagues within European law enforcement community and to our partners in the private industry for their input to the report.

Combining law enforcement and private sector insights allows us to present this comprehensive overview of the threat landscape.

The data collection for the IOCTA 2020 took place during the lockdown implemented as a result of the COVID-19 pandemic.

Indeed, the pandemic prompted significant change and criminal innovation in the area of cybercrime.

Criminals devised both new modi operandi and adapted existing ones to exploit the situation, new attack vectors and new groups of victims.

The threat landscape over the last year described in the IOCTA 2020 contains many familiar main characters.

The starring roles in terms of priority threats went to the likes of social engineering, ransomware and other forms of malware.

Several interviewees captured the essence of the current state of affairs of the threat landscape by stating: cybercrime is an evolution, not a revolution.

As time passes, the cyber-element of cybercrime infiltrates nearly every area of criminal activity.

Key elements mentioned in previous editions of the IOCTA that return this year merit more, rather than less, attention.

The repetition means the challenge still exists and has, in many cases, increased, underlining the need to further strengthen the resilience and response to well-known threats.

The IOCTA 2020 makes clear that the fundamentals of cybercrime are firmly rooted, but that does not mean cybercrime stands still.

Its evolution becomes apparent on closer inspection, in the ways seasoned cybercriminals refine their methods and make their artisanship accessible to others through crime as a service.

The COVID-19 crisis illustrated how criminals actively take advantage of society at its most vulnerable.

Criminals tweaked existing forms of cybercrime to fit the pandemic narrative, abused the uncertainty of the situation and the public's need for reliable information.

Across the board from social engineering to Distributed Denial of Service (DDoS) attacks and from ransomware to the distribution of child sexual abuse material (CSAM), criminals abused the crisis when the rest of society was trying to contain the situation.

The opportunistic behaviour of criminals during the pandemic, however, should not overshadow the overall threat landscape.

In many cases, COVID-19 caused an amplification of existing problems exacerbated by a significant increase in the number of people working from home.

This is perhaps most noticeable in the area of child sexual abuse and exploitation.

As in previous years, the amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has had serious consequences for the investigative capacity of law enforcement authorities.

In addition, livestreaming of child sexual abuse increased and became even more popular during the COVID-19 crisis; a recent case shows production also takes place in the EU.

Data compromise once more features as a central aspect throughout a number of threats. Both law enforcement and private sector representatives consistently report on social engineering among the top threats.

With regard to social engineering, in particular phishing, cybercriminals are now employing a more holistic strategy by demonstrating a high level of competency when exploiting tools, systems and vulnerabilities, assuming false identities and working in close cooperation with other cybercriminals.

However, despite the trend pointing towards a growing sophistication of some criminals, the majority of social engineering and phishing attacks are successful due to inadequate security measures or insufficient awareness of users.

In particular, as attacks do not have to be necessarily refined to be successful.

The developments in the area of non-cash payment fraud over the past twelve months reflect the overall increase in sophistication and targeting of social engineering and phishing.

Fuelled by a wealth of readily available data, as well as a Cybercrime-as-a-Service (CaaS) community, it has become easier for criminals to carry out highly targeted attacks.

As a result, law enforcement and industry continue to identify well established frauds as a major threat.

Subscriber identity module (SIM) swapping is one of the new key trends this year, having caused significant losses and attracted considerable attention from law enforcement.

As a highly targeted type of social engineering attack, SIM swapping can have potentially devastating consequences for its victims, by allowing criminals to bypass text message-based (SMS) two factor authentication (2FA) measures gaining full control over their victims' sensitive accounts.

Business Email Compromise (BEC) continues to increase.

As criminals are more carefully selecting their targets, they have shown a significant understanding of internal business processes and systems' vulnerabilities.

At the same time, certain other forms of fraud have entered the spotlight due to the sheer number of victims they have generated.

The spread of online investment fraud all over Europe is not necessarily new but has generated increased law enforcement attention as victims at

times lose their life savings to professional organised criminal groups that have incorporated cyber elements into their scams.

The clear majority of law enforcement respondents once again named ransomware as a top priority threat.

Although this point has been made in past editions of the IOCTA, ransomware remains one of the, if not the, most dominant threats, especially for public and private organisations within as well as outside Europe.

Considering the scale of damage that ransomware can inflict, victims also appear to be reluctant to come forward to law enforcement authorities or the public when they have been victimised, which makes it more difficult to identify and investigate such cases.

Criminals continued making their ransomware attacks increasingly targeted.

Ransomware has shown to pose a significant indirect threat to businesses and organisations, including in critical infrastructure, by targeting supply chains and third-party service providers.

Perhaps one of the most crucial developments is the new way of pressuring victims to pay by stealing and subsequently threatening to auction off victims' sensitive data.

Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases.

Criminals have converted some traditional banking Trojans into more advanced modular malware to cover a broader scope of functionality.

These evolved forms of modular malware are a top threat in the EU, especially as their adaptive and expandable nature makes them increasingly more complicated to combat effectively.

With a range of threat actors, this makes drawing general conclusions about particular threats challenging.

In areas ranging from social engineering and phishing, to ransomware and other forms of malware, law enforcement authorities witness a broad spectrum of threat actors.

These actors vary in terms of level of skill, capability and adaptability.

The top tier criminals manage to run their operations like a professional enterprise, whereas less sophisticated threat actors tend to rely on off-the-shelf materials to conduct their criminal activities.

The availability of the materials through CaaS, however, continues to make such activities accessible.

Moreover, across the board threat actors in different types of cybercrime demonstrate their resilience.

Perhaps more importantly, in areas such as the Darkweb, criminals have enhanced their cooperation and joined forces to provide a response to shared challenges.

This means they are able to make their business more robust and in particular incorporate better security solutions to ensure that law enforcement are unable to trace them.

Overall, cybercriminals are showing an improved level of operational security and proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies.

With cryptocurrencies, criminals also manage to complicate law enforcement's ability to trace payments connected to criminal activities.

To respond to the cybercrime challenges in a more effective manner, a number of key ingredients are essential.

First, information sharing is at the heart of any strategic, tactical and operational response regardless of the specific type of cybercrime.

Sharing information, which needs to be purposedriven and actionable, requires reliable coordination and cooperation from public and private partners.

At the same time, information sharing requires a legal framework and attitude that is sensitive to the timely exchange of information, which is crucial as cybercriminals can move their infrastructure within the blink of an eye.

This is particularly evident in the criminal abuse of the Darkweb, where short lifecycles of marketplaces influences law enforcement's ability to conduct investigations.

There is also the need to foster a culture of acceptance and transparency when organisations or individuals fall victim to cybercrime.

Re-victimising victims after a cyber-attack is counterproductive and a significant challenge, as law enforcement need companies and individuals who have been subject of a crime to come forward.

This can help resolve the challenges in reporting we currently face. Besides information sharing through enhanced coordination and cooperation, other key elements to include in an effective response are prevention and awareness and capacity building.

We can reduce the success rate of many forms of cybercrime by educating individuals and organisations in recognising criminal activity before they fall victim to it.

It is worth underlining the importance of the responsibility of industry in integrating security and privacy in their design as fundamental principles, instead of shaming end users as the weakest link.

Through capacity building, on the other hand, law enforcement across different crime areas will be able to understand and respond to the cyber-element of crimes.

Finally, taskforce work such as coordinating and de-conflicting law enforcement operational response, for which the Europol Joint Cybercrime Action Taskforce (J-CAT) platform is vital, continues to play a key role in the current cybercrime landscape.

The report:
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Number 7

A solution to every puzzle

John C Williams, President and Chief Executive Officer of the Federal Reserve Bank of New York, at the 2020 US Treasury Market Conference

Good morning, everyone, and welcome to the sixth annual U.S. Treasury Market Conference.

I wish we were able to meet in person at the New York Fed. But, while the location for this year's conference may have moved from an auditorium to your living room, the goal remains the same: To bring together market participants and representatives from five public sector bodies-the New York Fed, the Board of Governors, the Treasury, the SEC, and the CFTC. And, the events of the past year make the conversations we will have today all the more valuable and timely.

Today, I'd like to begin with stressing the importance of well-functioning financial markets and then look at two recent episodes of volatility and the lessons learned.

I'll close by explaining the Fed's role to support functioning in this critical part of the financial system.

At last year's conference, I spoke about the transition away from LIBOR. Because I am certain all of you have committed to memory everything I said then, I'll keep my remarks on LIBOR today short and to the point: We have only 459 days until the availability of LIBOR can no longer be assured, and everyone needs to put their nose to the grindstone in their efforts to prepare for the move off LIBOR. In the immortal words of Captain Jean Luc Picard-make it so!

Before I continue on to today's topic or quote other favorite Star Trek characters, I need to give the standard Fed disclaimer that the views I express today are mine alone and do not necessarily reflect those of the Federal Open Market Committee or others in the Federal Reserve System.

The Heart of the Economy

The markets that are the center of attention today-the Treasury market, the repo market, and the mortgage-backed securities market-represent the heart of the circulatory system of our financial system and our economy, and indeed the global economy.

When they are working smoothly, all the other parts of the system can perform as they should.

But, the opposite is true as well. If these critical markets break down, credit stops flowing, and people can't finance the purchase of a car or a home, businesses can't invest, and the economy suffers, resulting in lost jobs and income.

Financial markets aren't static-they evolve over time in response to changes in technology, regulation, and business models.

The Treasury market is not immune to this process of change.

We have seen the emergence of principal trading firms, changes in regulations of key intermediaries, and the growth of nonbank financial institutions.

With this evolution, it is vitally important to ensure that safeguards and systems also evolve so that these markets function well in all circumstances and conditions, including unprecedented events like the pandemic.

We need to reflect on and learn from these experiences and consider ways to make these and other markets more robust, thereby minimizing the potential negative consequences to the economy and the need for extraordinary policy responses.

Market Conditions in September and March

I know it might seem like a lifetime ago, but allow me take you to mid-September of last year.

A number of otherwise ordinary occurrences-including corporate tax payments and settlement of newly issued Treasuries-were expected to put some upward pressure on short-term rates, but the market response was out of proportion to the magnitude of the shock.

Conditions in funding markets became highly volatile, with both secured and unsecured lending rates rising sharply.

Indeed, the size of the reaction in repo rates, the spillover to the federal funds market, and the emergence of strains in market functioning were well outside of recent experience. And the market stress was looking to get worse, not better.

In response to these developments, the Federal Reserve conducted a series of large-scale repo operations with the aim of calming conditions in funding markets and bringing the federal funds rate within the target range.

The provision of liquidity had the desired effect of reducing strains in markets, narrowing the dispersion of rates, and keeping the federal funds rate within the target range.

Moving to more recent events, in March of this year the global spread of the pandemic led to a rapid and massive movement of funds around the world as investors sought to protect themselves from the highly uncertain and darkening economic outlook.

These flows threatened to overwhelm the financial system and resulted in intense strain and disruption in short-term funding markets and markets for Treasury securities and agency mortgage-backed securities.

Measures of market functioning deteriorated to levels near, or in some cases worse than, those we saw at the peak of the 2008 global financial crisis.

In response to the extraordinary volatility and signs of market disruption caused by the pandemic, the Federal Reserve greatly expanded its repo operations and decisively and immediately began purchasing enormous quantities of U.S. Treasury securities and agency mortgage-backed securities.

Our approach was to deliver a rapid and overwhelming response that would give assurance to market participants that liquidity would be there in the coming days and months.

These actions, combined with the introduction of emergency lending facilities to provide liquidity to funding and credit markets, proved successful.

They quickly restored market functioning and averted what could have been a much more severe pullback from markets and the flow of credit to households and businesses.

Indeed, the rapid restoration of market functioning helped restore a robust flow of credit at historically low interest rates to the economy, which has provided a boost for the recovery.

To read more: https://www.bis.org/review/r201001e.htm

Number 8

Speech at the Congress of the Association of Banks of Russia

Elvira Nabiullina, Governor of the Bank of Russia, at the Congress of the Association of Banks of Russia, Moscow.

Good afternoon colleagues and Mr Aksakov,

I am delighted to welcome all attendees to the congress - both those here in the hall and those joining us by video conference.

Coronavirus continues to have an effect on our lives. And it is already clear that it will have long-term repercussions. The way people and businesses behave has changed and all this, of course, will have an effect on the banking business as well. We are now at the point where we need to assess these changes, adapt to them, and find new areas of growth.

I must say that in general the Russian banking system is coping with all the challenges.

What worked and helped us come through the most acute phase of the pandemic: reinforcing the resilience of financial institutions - the capital cushion, liquidity cushion, and most importantly, a more responsible approach taken by banks to credit risk, the macroprudential buffers that had been accumulated, and the dedollarisation of banks' balance sheets, which has reduced the risks associated with exchange rate fluctuations.

All this ensured that banks were able to support their customers and carry on lending at the same time.

Of course, the regulatory easing also played a role: it gave banks the chance to pass through this period more easily.

But what fundamentally distinguishes today's situation from, say, that of 2014-2015 is that regulatory easing was, in fact, just one additional comfort factor in a period of difficult conditions, and not "the last chance" or the only way to stay afloat.

Undoubtedly, in the conditions of the epidemic, it helped greatly that Russian banks boast a high level of digitalisation.

Almost all services were available online, and of those in demand on a daily almost all were available. Even before the epidemic, most banking customers extensively used remote services, but even those who previously rarely used remote services started using them without great difficulty.

In my speech today, I would like to focus on two clusters of issues. The first deals directly with the impact the epidemic had on the banking business, the current situation, and the measures we are taking to ensure that going forward banks are resilient in their operations.

The second concerns what comes next, how to develop the banking business with allowance for the long-term repercussions of the pandemic.

How does the current situation look?

In the last few months, we have seen a gradual recovery in business activity, the financial markets are stabilising, and lending is also recovering. It has to be said that the economy shrunk less than many expected.

The recovery may be uneven, but it is proceeding broadly in line with our forecasts. In particular, this can be seen in our monitoring of sectoral financial flows, which we started conducting during the pandemic.

We can see that deviations from the normal level of payments vary by industry, fluctuating from week to week, but the overall trend towards normalisation is undeniable.

For example, in the last week, the total deviation of incoming payments down from the normal level was –7.1% compared to –7.3% the week before. But excluding mining, the production of petroleum products, and government activities, the deviation also decreased to total –1% after –4.4% a week earlier.

The Bank of Russia transitioned to a loose monetary policy, cutting its key rate to 4.25% - a historic low.

This is necessary to keep inflation on target against the backdrop of disinflationary risks linked with a significant drop in aggregate demand. But this monetary policy focus will also help the economy return to potential more quickly.

That said, it is important to take into account that the structural changes in both the Russian and global economy, generated by the pandemic, have most likely affected the potential of the economy. How extensively - it remains to be seen and evaluated.

The banking sector is supporting recovery processes: corporate loans have grown by 5.5% since the beginning of the year (growth was only 5.8% last year).

Of course, this is also because companies that experienced a sharp drop in revenue experienced a need for debt financing. But the banking sector overall has continued to lend, and we estimate that lending growth will be up to 9% this year.

At the beginning of the pandemic, we launched a preferential refinancing programme for banks lending to SMEs. Now Mr Aksakov has suggested that we review these decisions.

But I would like to remind you that we needed to ensure that small businesses had access to funding as fast as possible during the pandemic. 409 billion rubles were taken out of the limit.

But I would like to say that this program will be phased out gradually over the course of a year. However, at the same time, we are extending the operation of this instrument (it will be possible to obtain preferential refinancing until September 30).

Why? Because rate cuts after the transition to a loose monetary policy and measures of government support for SMEs bring about sufficient lending potential in this segment. It really was a rapid-response anti-crisis measure.

How do borrowers feel now? The restructuring programmes have helped them withstand the shock of Q2.

Undoubtedly, it is important to understand that some borrowers may not cope with the repercussions of the epidemic, and we can see that banks have already been carefully evaluating borrowers' business and loans have been available for more efficient businesses.

And despite the stress, there has not been significant loan impairment as was the case in 2014-2015.

The share of non-performing and bad loans in H1 2020 in the corporate portfolio increased slightly (by 0.1 p.p. to 11.1%).

In the future, of course, problems may "catch up" with borrowers in those industries where demand is recovering more slowly, both because of the restrictions and because of the change in people's behaviour. But in general, the situation does not currently look too alarming.

Retail lending is also gradually recovering: after a decline in April and stagnation in May, the growth rate in June-July reached almost pre-coronavirus levels.

In contrast to 2019, most of the growth comes from the mortgage sector thanks in large part to the Government's preferential programs. For example, in June they covered about 45% of all mortgage loans issued.

Specifically, more than a third (37%) were covered by the "6.5 Programme". Since the beginning of the year, the retail portfolio on the whole has grown 6%. During the same period last year, growth stood at 11%.

However, back then the main driver was unsecured loans.

At the end of 2020, we expect retail portfolio growth to be up to 9% as well. That said, the growth structure of retail lending (more mortgages, fewer unsecured loans) is a positive factor.

During the pandemic, some households experienced a sharp temporary decline in income, which is linked with an increased debt burden on borrowers.

To ensure that this situation does not increase pressure on banks' capital, we have reduced macroprudential buffers by 30-50 percentage points.

The maximum reduction is for borrowers with a low debt burden, so that the recovery of retail lending occurs without a dangerous increase in household debt overburden.

Arrears grew more in the retail loan portfolio than in the corporate portfolio but also moderately - from 6.6 to 7.9%. Impairment was mostly seen in unsecured loans, while mortgage quality has remained consistently high.

At the same time, non-performing loans are well covered by reserves (more than 75%).

Significant loan impairment was avoided thanks to numerous support measures for borrowers by the Government and support measures for banks, and the easing of the reserves on restructured loans adopted by the Central Bank.

Since the start of the pandemic, banks have restructured within the framework of their programs as well as repayment holidays about 10% of the total portfolio; the significant amount of 1.5 trillion Mr Aksakov referred to mostly concerns small and medium businesses and individuals.

And if you take all the restructuring that banks carried out on large loans and large enterprises - it comes to more than 5 trillion, i.e. it is a rather large amount of restructuring.

Its peak was in May, and as of July there has been a steady decline in the demand for restructuring from borrowers, which also suggests there is a normalisation and gradual recovery of economic activity.

Restructuring was really important during the most serious period of the pandemic when a significant chunk of businesses ceased operating and many people's incomes declined.

We have permitted that reserves on such loans may temporarily not be increased so that banks can carry out this large-scale, really large-scale, programme, spread losses over time, and enable businesses and households to regain their creditworthiness.

But in the short term, I urge banks to do this. Banks must assess the real loan portfolio quality. It is very important that the recognition of losses on non-refundable loans is not overly delayed.

I understand that banks will want to drag out this regulatory easing, but "delaying" the recognition of losses can lead to banks not being able to direct resources to lending to effective companies.

Having non-performing assets on the balance sheet reduces investor confidence.

There are many examples in global practice where there was a delay in recognising bad assets: the "lost decade" in Japan in the 90s, the situation in a number of European countries following the global financial crisis of 2007-2009, and our own experience in 2008-2009.

Therefore, we have decided to gradually phase out regulatory easing. We will really phase it out, as Mt Aksakov has urged, carefully. But the phase-out is necessary.

And the banks that made use of the easing will have to build up reserves in full for loans to large companies by 1 April next year, and for household

loans and loans to SMEs - by 1 July next year within a timeline convenient to them.

Banks can also use capital that has been formed to meet capital adequacy buffers but with appropriate restrictions on profit distribution.

We generally recommend that banks take a particularly judicious approach to paying dividends as there is continued uncertainty linked to the pandemic and capital may be required in the future to absorb losses.

Therefore, before paying dividends, it is vital to assess future capital needs based on conservative estimates.

Now about the funding situation. It has also levelled out. In general, over the first seven months of 2020, the funds of legal entities increased by almost 3% (by 2.9%). Concurrently, there was a significant inflow (+27%) of funds of state organisations.

Household contributions during this period demonstrated divergent dynamics. At the start of the pandemic, especially in March, there was an outflow of funds (people formed cash reserves at the outset of the lockdown period). However, as early as June-July, the situation had stabilised.

On the one hand, this is due to the peak of the epidemic passing and the gradual recovery of people's income, and, on the other hand, the substantial support provided by the Government's welfare payments.

The active growth of funds in escrow accounts (more than 330 billion rubles since the beginning of the year) lent additional support, and this is noticeable, to deposits, thanks to the development of project financing for housing construction.

Therefore, this year deposits have already increased by 514 billion rubles in the banking system, or 1.6%. The overall level of liquidity in the system remains high.

And against the backdrop of monetary policy easing, deposit rates have declined in the corporate segment by 1.3p.p. and in the retail segment by 0.8 percentage point since the beginning of the year.

This allows banks to lend at lower rates without losing too much of their margins. But there is a flip side of the coin here too: it affects the attractiveness of deposits versus other forms of savings.

This year we have seen a record flow of retail funds into alternative savings instruments, and capital market instruments.

In general, this flow does not affect the total amount of savings in the economy, or their availability as a resource base for investments.

But banks, when determining their policy on deposit rates, need to take into account this growing competition from the securities market and other instruments.

And in the structure of the deposit products they offer, accommodate for the fact that over a medium-term horizon, as disinflationary factors and disinflationary risks are exhausted, a return to neutral monetary policy is inevitable.

Now about banking sector profit -- in the first 7 months of this year it stood at 761 billion rubles (return on capital - about 13% year on year). That said, of course, it is necessary to consider that more than 70% of this profit was made in Q1, while in Q2 profit fell to 102 billion rubles.

It is difficult to make profit forecasts right now. However, in light of the normalisation of the economic situation, the extension of a number of easing measures and the timetable for additional provisioning, a profit this year of about 1 trillion seems achievable.

The fact that most banks maintain profitability (in general, the proportion of unprofitable banks has probably not changed significantly during the pandemic and in general the share of assets of unprofitable banks in the assets of the banking sector is now about 5%, i.e., in general, the share of unprofitable banks is not very large).

All of this allows banks to ramp up lending and maintain capital reserves. In general, the overall sector's capital reserves, measured against key capital ratios, stand at about 5.9 trillion rubles.

This is enough to reserve, if necessary, an additional approximately 11% of banking sector lending, which is a very serious safety margin.

That is, suppose even if about a third of those restructured loans end up defaulting (which is not a small amount), the capital reverses cover this amount threefold. Let me clarify that this is an overall sector estimate. Capital reserves are unevenly distributed among banks.

What general conclusion can be drawn from the response to the pandemic by the banking sector and the implementation of our measures?

You cannot predict exactly what the next shock will be, when it will be, what it will be, but reducing financial stability risks, creating safety nets, and consistently eliminating vulnerabilities in the financial sector, will offer protection in any case. And you and I are sure of this. Therefore, of course, maintaining financial sector stability as a whole is a priority of our policy.

To read more: https://www.bis.org/review/r201001f.htm

Number 9

Cloud Security: The way forward?

National Cyber Security Centre

A survey completed by over 200 UK organisations, showed that moving to a cloud-based IT environment had saved them from collapse due to the increased demand for remote working availability as a result of the COVID-19 pandemic.

You may visit:
https://www.centrify.com/about-us/news/press-releases/2020/cloud-adoption-has-saved-more-half-uk-businesses-covid-19

However, the pandemic has also highlighted the potential weaknesses in IT security, with more than half of the businesses polled seeing an increase in hijack attempts on employee accounts and impersonation attacks becoming harder to detect.

You may visit:
https://www.mimecast.com/content/impersonation-attack/#:~:text=An%20impersonation%20attack%20is%20a,login%20credentials%20that%20attackers%20can

Further analysis from security experts has warned of the increased chance of remote workers falling victim to cyber attacks. This is largely due to inadequate security protection installed on personal devices and home broadband routers or workers becoming 'distracted' and clicking on harmful links.

The NCSC has further reading to help answer security concerns about moving to a cloud-based IT solution, guidance to help you determine how confident you can be that a cloud service is secure enough to handle your data and information to increase awareness about email security. You may visit:
https://www.ncsc.gov.uk/blog-post/why-cloud-first-is-not-a-security-problem

Number 10

NIST Crowdsourcing Challenge to De-Identify Public Safety Data Sets

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 launched a crowdsourcing challenge to spur new methods to ensure that important public safety data sets can be de-identified to protect individual privacy.

The Differential Privacy Temporal Map Challenge includes a series of contests that will award a total of up to $276,000 for differential privacy solutions for complex data sets that include information on both time and location.

For critical applications such as emergency planning and epidemiology, public safety responders may need access to sensitive data, but sharing that data with external analysts can compromise individual privacy.

Even if data is anonymized, malicious parties may be able to link the anonymized records with third-party data and re-identify individuals. And, when data has both geographical and time information, the risk of re-identification increases significantly.

"Temporal map data, with its ability to track a person's location over a period of time, is particularly helpful to public safety agencies when preparing for disaster response, firefighting and law enforcement tactics," said Gary Howarth, NIST prize challenge manager. "The goal of this challenge is to develop solutions that can protect the privacy of individual citizens and first responders when agencies need to share data."

Differential privacy provides much stronger data protection than anonymity; it's a provable mathematical guarantee that protects personally identifiable information (PII). By fully de-identifying data sets containing PII, researchers can ensure data remains useful while limiting what can be learned about any individual in the data regardless of what third-party information is available.

The individual contests that make up the challenge will include a series of three "sprints" in which participants develop privacy algorithms and compete for prizes, as well as a scoring metrics development contest (A Better Meter Stick for Differential Privacy Contest) and a contest designed

to improve the usability of the solvers' source code (The Open Source and Development Contest). The challenge is being hosted by NIST's Public Safety Communications Research (PSCR) division and managed by DrivenData and HeroX.

The Better Meter Stick for Differential Privacy Contest will award a total prize purse of $29,000 for winning submissions that propose novel scoring metrics by which to assess the quality of differentially private algorithms on temporal map data.

The three Temporal Map Algorithms sprints will award a total prize purse of $147,000 over a series of three sprints to develop algorithms that preserve data utility of temporal and spatial map data sets while guaranteeing privacy.

The Open Source and Development Contest will award a total prize purse of $100,000 to teams leading in the sprints to increase their algorithm's utility and usability for open source audiences.

To learn about eligibility requirements, visit challenge.gov, and for additional information about the challenge, visit DrivenData.org.

NIST, a nonregulatory agency of the U.S. Department of Commerce, promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

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.

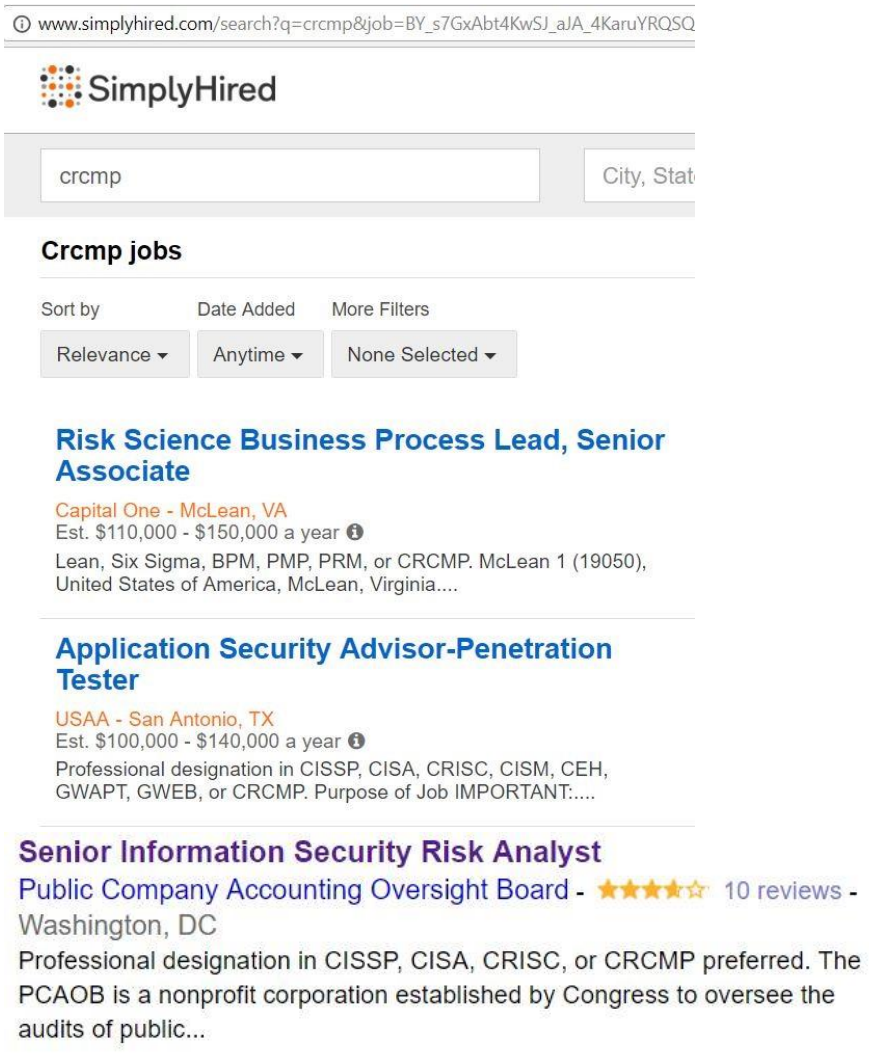
International Association of Risk and Compliance Professionals

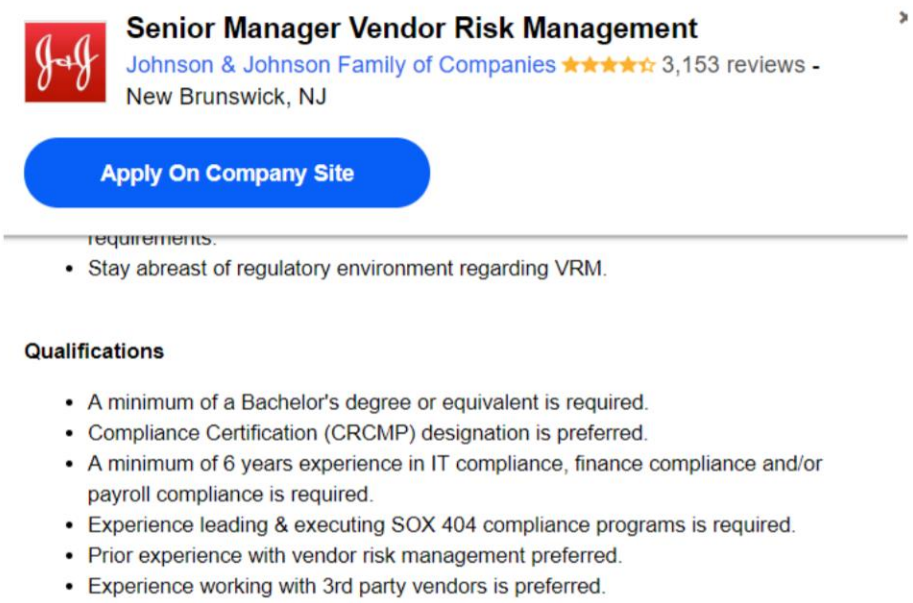
You can explore what we offer to our members:

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





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html