Monday, June 14, 2021

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,

This summer we will read an interesting paper about the Federal Reserve Board's current thinking on *digital payments,* with a particular focus on the benefits and risks associated with *central bank digital currencies (CBDCs)*. Today we can have a feeling about the content of this paper.

Lael Brainard, Member of the Board of Governors of the Federal Reserve System, gave an interesting presentation at the Consensus by CoinDesk 2021 Conference in Washington DC, with title *"Private money and central bank money as payments go digital - an update on CBDCs"*

She said: "there is a risk that the widespread use of private monies for consumer payments could fragment parts of the U.S. payment system in ways that impose burdens and raise costs for households and businesses."

She also said: "A predominance of private monies may introduce consumer protection and financial stability risks because of their potential volatility and the risk of run-like behavior.

Indeed, the period in the nineteenth century when there was active competition among issuers of private paper banknotes in the United States is now notorious for inefficiency, fraud, and instability in the payments system. It led to the need for a uniform form of money backed by the national government."

Lael Brainard explained that a stablecoin is a type of digital asset whose value is tied in some way to traditional stores of value, such as government-issued, or fiat, currencies or gold. Stablecoins vary widely in

the assets they are linked to, the ability of users to redeem the stablecoin claims for the reference assets, whether they allow unhosted wallets, and the extent to which a central issuer is liable for making good on redemption rights.

Unlike central bank fiat currencies, stablecoins do not have legal tender status. Depending on underlying arrangements, some may expose consumers and businesses to risk.

If widely adopted, stablecoins could serve as the basis of an alternative payments system oriented around new private forms of money.

Read more at number 10 below. Welcome to our Top 10 list.

Best regards,

George Lekatis

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)

Can Digital Identity Solutions Benefit from Blockchain Technology?

The knowledge building seminar organised by the EU Agency for Cybersecurity explores the possible applications of blockchain technology in the field of digital identity and online trust.

Number 2 (Page 7)

The money laundering business – making dirty money look clean

How criminals use banks to launder money and how good banks are at protecting themselves from such criminal activities.

Number 3 (Page 12)

United States Government Accountability Office

Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market

Number 4 (Page 15)

Breaking the Specification: PDF Certification

RUHR-UNIVERSITÄT BOCHUM

Simon Rohlmann, *Ruhr University Bochum*, simon.rohlmann@rub.de
Vladislav Mladenov, *Ruhr University Bochum*, vladislav.mladenov@rub.de
Christian Mainka, *Ruhr University Bochum*, christian.mainka@rub.de
Jörg Schwenk, *Ruhr University Bochum*, joerg.schwenk@rub.de

Number 5 (Page 17)

Market entry: Information regarding the authorisation procedure for banks and financial services providers on bafin.de now available in English

Number 6 (Page 19)

The Green Swan Conference - Coordinating finance on climate Watch the livestream

Number 7 (Page 21)

Cyber resilience practices - Executive Summary

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

Number 8 (Page 23)

Whom do consumers trust with their data? US survey evidence

Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster and Kelly Shue

BIS

Number 9 (Page 26)

Another Nobelium Cyberattack

Tom Burt, Corporate Vice President, Customer Security & Trust

Microsoft

Number 10 (Page 29)

Private money and central bank money as payments go digital - an update on CBDCs

Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Consensus by CoinDesk 2021 Conference, Washington DC

Number 1

Can Digital Identity Solutions Benefit from Blockchain Technology?

The knowledge building seminar organised by the EU Agency for Cybersecurity explores the possible applications of blockchain technology in the field of digital identity and online trust.

What is blockchain technology used for?

Blockchain technology was first introduced as a technology for digital currencies, but recently new application areas are emerging. There are proposals to use blockchain technology for electronic voting and secure sharing of medical data. Besides, there is now a booming market of NFTs (non-fungible tokens) underpinned by blockchain technology.

A new field, which could also benefit from blockchain technology is digital identities. Resorting to blockchain-based digital identity frameworks would allow users greater control over their identity data, and at the same time offer a resilient and decentralised system without single points of failure.

Who was the seminar intended for?

Organised by the EU Agency for Cybersecurity (ENISA) in collaboration with the Delft Blockchain Lab of the Dutch Delft University of Technology, the knowledge building seminar held today was intended for national authorities overseeing the trust services market and for authorities involved with digital identity schemes.

This seminar was organised in the context of ENISA's support of the ENISA Article 19 Expert Group, a working group of national authorities supervising the trust service providers in the EU.

What did the seminar focus on?

The seminar introduced the basic concept of blockchain technology, and explored its application in the area of trust services and electronic identification, making a comparison with traditional centralised hierarchical ones in terms of user control and single points of failure. The focus here was on advantages and disadvantages, potential abuse and misuse, potential impact on society and the economy as well as the issue of governance.

The seminar concluded with an overview of several existing initiatives, such as the European Blockchain Services Infrastructure (EBSI), Sovrin, and the TU Delft Trustchain. It also included an overview of real-life scenarios, such as controlling access to a construction site and the confirmation of diplomas by a university.

About ENISA's knowledge building seminars

This seminar is part of a broader series of knowledge building seminars that ENISA organises for national authorities in the EU on new technologies and the cybersecurity opportunities and risks associated with them. Previous seminars for authorities covered topics such as cloud security, internet backbone security and applications of cryptography.

To learn more:
https://www.blockchain-lab.org/#aboutus

https://resilience.enisa.europa.eu/article-19

Number 2

The money laundering business – making dirty money look clean

How criminals use banks to launder money and how good banks are at protecting themselves from such criminal activities.

BaFin Federal Financial Supervisory Authority

Thomas B. runs a restaurant, but business is not exactly thriving. Five tables and only a handful of guests at the best of times. Yet astonishingly enough he is still able to pay in huge amounts of cash at his bank every Monday and Thursday. Not only friends and neighbours find this a little surprising. The bank employee is equally puzzled whenever B. turns up at the bank in a glamorous limousine.

He broaches the subject with the customer, curious to know how it is that B. regularly pays in such high amounts of money when he has hardly any guests. The bank steps into action in response to a kind of warning system set up by credit institutions in order to track down suspicious transactions.

By now, Thomas B. should be feeling nervous, because the money did not come from his restaurant's culinary delights but from a thriving drug trade. For a long time, his main problem has been finding ways to dispose of all that cash and channel the illicit funds into the legal economic system without attracting attention.

This is where the restaurant comes into play. The only reason he is running it is to conceal the source of his income and make the dirty money look clean. There is just one thing he overlooked – huge earnings and a poorly frequented restaurant simply do not add up. The bank noted this discrepancy, and reported it to the Financial Intelligence Unit (FIU) of the German customs authorities.

This case is purely fictional, but things like this do happen, time and again. And the channels through which the funds flow are often far more convoluted and difficult to trace.

Al Capone and his laundromats

Al Capone was the first to launder money in this way, but not with restaurants. The legendary gangster invested the profits from criminal activities such as prostitution, racketeering, illegal gambling and alcohol trading in a whole chain of laundromats. Capone, who it is claimed never had a bank account, managed to conceal his proceeds by maintaining that they were earnings from the laundromats.

Whether this is fact or mere fiction is unclear. When asked about the source of his earnings at the trial in Chicago in 1931, Capone allegedly replied that he was "in the laundering business". In any case, it is safe to say that he was probably the first to coin the term "money laundering". Although this ploy failed to spare him a term in prison, he was not sentenced for murder or blackmail – none of which could be proved against him – but for tax evasion.

Nowadays, criminal investigators have more efficient tools for exposing tricks of this kind, thanks not least to BaFin and the FIU. Banks are obliged to notify the FIU if they regard customers or payments as suspicious. The FIU follows up on these suspicious transaction reports (STRs) and analyses them.

Money laundering prevention during the pandemic

BaFin for its part is responsible for monitoring whether the institutions of the financial sector under its supervision are adequately protecting themselves against being abused for money laundering purposes.

Normally, teams from BaFin travel to the institutions in order to gain an impression on-site of the quality of the institutions' anti-money laundering (AML) measures. This has become much more difficult since the outbreak of the coronavirus pandemic.

But cancelling the inspections because of the pandemic was out of the question. "From April 2020, we initially conducted our inspections by telephone and then very quickly developed remote solutions which could also be used when working from home", explained Dr Thorsten Pötzsch, BaFin's Chief Executive Director also responsible for money laundering prevention.

Following a brief period in the summer, when it was possible to conduct on-site inspections at least subject to certain restrictions, remote inspections then became the norm.

The usual difficulties with lines engaged or microphones and cameras not working properly had been overcome by then and the inspection priorities adapted to take account of a remote working environment. For example, the main focus was placed on risk analysis, questions regarding the AML officer functions and the STR procedure.

BaFin tracks down errors

The inspections were successful. BaFin detected errors, particularly in the institutions' risk analyses, some of which were serious. The institutions had failed to correctly determine and evaluate AML risks.

BaFin's supervisors also identified shortcomings in the suspicious transactions reported by the institutions, although these were generally less serious.

Moreover, many institutions had failed to document cases in accordance with the specifications under the German Money Laundering Act (Geldwäschegesetz – GwG), which made it difficult for BaFin to understand why certain decisions were taken.

At some institutions, BaFin examined the procedure for establishing and verifying the identity of customers, which is crucial in the prevention of money laundering.

It transpired that the institutions had made errors here, too, albeit less when identifying the customers themselves than when establishing the identity of beneficial owners, or persons used by a customer as a representative or messenger for the bank.

But errors had also been made in the identification procedure for politically exposed persons (PEPs). This group of persons includes heads of state, heads of government, ministers, members of the European Commission, members of parliament and constitutional judges to whom particularly strict AML provisions apply.

The inspections also revealed that a number of institutions had failed to update their customer data in due time. A by-product of the inspections was the realisation that many institutions were saving money in the wrong places and should be investing more in IT and in staff.

"Not all institutions are where they should be", said Pötzsch, but an awareness for money laundering has been developed. There has been a sharp rise in the number of suspicious transactions reported to the FIU in recent years, with more than 90 percent of these reports deriving from those sections of the financial sector under BaFin's supervision. Pötzsch notes that institutions and authorities have become more vigilant. "All parties involved are now also far better networked within Germany", he adds, referring to the Anti Financial Crime Alliance (AFCA).

BaFin, the FIU and 14 banks have joined forces in this alliance to address the problem of money laundering (see expert article on the BaFin website dated 18 November 2019).

Plans for the times after the pandemic

When asked how BaFin expects the inspections to be conducted this year, Pötzsch gave a cautious response. “We don’t know how the pandemic will develop and when we will be able to conduct on-site inspections again. One thing is certain – in 2020, we were unable to inspect all the priority areas in the way we had intended. But nothing will be omitted.“ BaFin will also deal in-depth with a number of issues, in particular the crypto currency business of institutions, the money-remittance business and the procedure for reporting suspicious transactions.

BaFin is therefore still conducting its inspections off-site and is unlikely, as things currently stand, to return completely to the old system of inspections.

On the one hand, the teams prefer to be present in the institutions’ offices as they find the personal contact with the employees important.

On the other hand, the pandemic has shown that remote inspections are possible.

There is one other positive aspect to consider – the teams do not need to travel anywhere and they have more time for the actual inspection. Pötzsch could therefore envisage combining the two forms of inspection in the future – depending on the risk of the institution and inspection priorities.

Money laundering prevention across the EU

The EU Commission plans to present several proposals for more effective joint action against money laundering in Europe. The proposals are expected to mainly concern the enforcement of standard rules applicable throughout the entire EU. There is also talk of setting up a central European anti-money laundering supervisor.

“What we need is a truly harmonised European legal framework – a regulation that is directly applicable, not just directives that grant the member states too much leeway for implementation, as in the past”, said Pötzsch.

A patchwork of supervisory practices will not adequately equip supervisors to combat money laundering effectively, much less prevent it.

The Chief Executive Director is confident that the negotiations will be completed by the end of 2022 and that the regulation will be approved and

the legal foundations thus laid for a European anti-money laundering authority.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2103_GW_Fallkonstellationen_en.html

Number 3

United States Government Accountability Office

Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market

What GAO Found

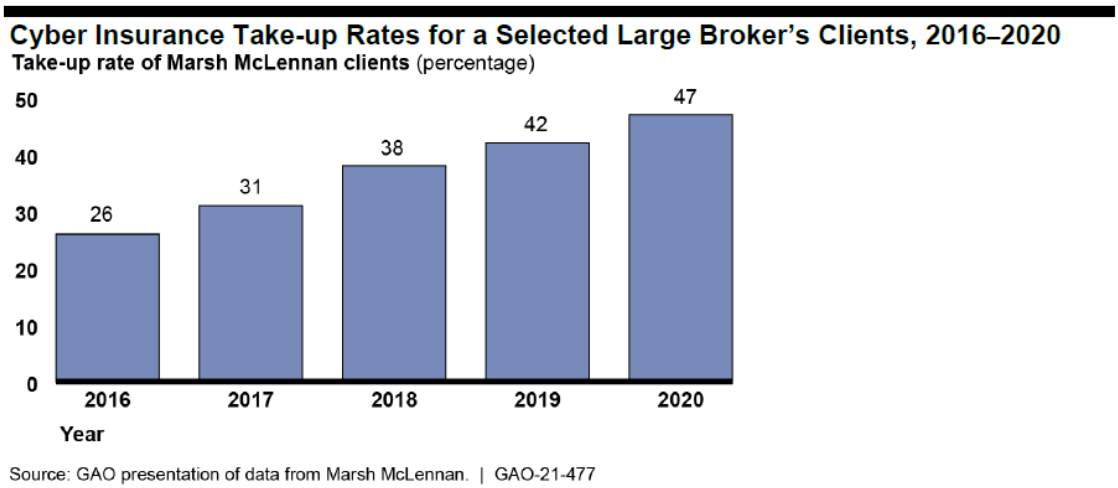
Key trends in the current market for cyber insurance include the following:

• *Increasing take-up*. Data from a global insurance broker indicate its clients' take-up rate (proportion of existing clients electing coverage) for cyber insurance rose from 26 percent in 2016 to 47 percent in 2020 (see figure).

• *Price increases*. Industry sources said higher prices have coincided with increased demand and higher insurer costs from more frequent and severe cyberattacks. In a recent survey of insurance brokers, more than half of respondents' clients saw prices go up 10–30 percent in late 2020.

• *Lower coverage limits*. Industry representatives told GAO the growing number of cyberattacks led insurers to reduce coverage limits for some industry sectors, such as healthcare and education.

• *Cyber-specific policies*. Insurers increasingly have offered policies specific to cyber risk, rather than including that risk in packages with other coverage. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.



Source: GAO presentation of data from Marsh McLennan. | GAO-21-477

The cyber insurance industry faces multiple challenges; industry stakeholders have proposed options to help address these challenges.

• *Limited historical data on losses*. Without comprehensive, high-quality data on cyber losses, it can be difficult to estimate potential losses from cyberattacks and price policies accordingly. Some industry participants said federal and state governments and industry could collaborate to collect and share incident data to assess risk and develop cyber insurance products.

• *Cyber policies lack common definitions*. Industry stakeholders noted that differing definitions for policy terms, such as "cyberterrorism," can lead to a lack of clarity on what is covered. They suggested that federal and state governments and the insurance industry could work collaboratively to advance common definitions.

Background

A cyber incident is defined as a cyber event that jeopardizes the cybersecurity of an information system or the information the system processes, stores, or transmits; or an event that violates security policies, procedures, or acceptable use policies, whether resulting from malicious activity or not.

Cyber incidents, including cyberattacks, can damage information technology assets, create losses related to business disruption and theft, release sensitive information, and expose entities to liability from customers, suppliers, employees, and shareholders.

Some private insurance companies offer businesses and other entities cyber insurance to protect against first-party (policyholder) and third-party losses (policyholder's clients or customers) from an event that jeopardizes the confidentiality, integrity, and availability of an information system.

The insurance can be provided through a standalone policy that provides only cyber insurance coverage or as a part of a package policy that provides multiple types of coverage, such as a general commercial liability insurance policy.

States regulate the private insurance market, including for cyber insurance.

The regulators seek to ensure that insurance policy provisions comply with state law, are reasonable and fair, and do not contain major gaps in coverage that might be misunderstood by consumers and leave them unprotected.

States generally do not establish minimum standards for cyber insurance policy coverage; they largely have focused on the solvency of cyber insurers, according to NAIC.

Some states and NAIC have promoted cybersecurity and data protections for insurers.

The Federal Insurance Office in Treasury administers the Terrorism Risk Insurance Program (TRIP), which requires the federal government to share some losses with private insurers in the event of a certified act of terrorism. Losses from cyberattacks might be reimbursed under TRIP if the attacks met certain certification criteria specified by the program.

We will be issuing a report later in 2021 that examines

(1) the risks and costs of cyberattacks on U.S. critical infrastructure;

(2) insurance coverage that is available for losses related to cyber risk, including cyberterrorism; and

(3) the extent to which TRIP, under the Terrorism Risk Insurance Act (TRIA), is structured to respond to cyberattacks and cyberterrorism.

To read more: https://www.gao.gov/assets/gao-21-477.pdf

Number 4

Breaking the Specification: PDF Certification

RUHR-UNIVERSITÄT BOCHUM

Simon Rohlmann
Ruhr University Bochum
simon.rohlmann@rub.de

Vladislav Mladenov
Ruhr University Bochum
vladislav.mladenov@rub.de

Christian Mainka
Ruhr University Bochum
christian.mainka@rub.de

Jörg Schwenk
Ruhr University Bochum
joerg.schwenk@rub.de

Abstract

The Portable Document Format (PDF) is the defacto standard for document exchange.

The PDF specification defines two different types of digital signatures to guarantee the authenticity and integrity of documents: approval signatures and certification signatures.

Approval signatures testify one specific state of the PDF document. Their security has been investigated at CCS'19.

Certification signatures are more powerful and flexible. They cover more complex workflows, such as signing contracts by multiple parties.

To achieve this goal, users can make specific changes to a signed document without invalidating the signature.

This paper presents the first comprehensive security evaluation on certification signatures in PDFs. We describe two novel attack classes – Evil Annotation and Sneaky Signature attacks which abuse flaws in the current PDF specification.

Both attack classes allow an attacker to significantly alter a certified document's visible content without raising any warnings.

Our practical evaluation shows that an attacker could change the visible content in 15 of 26 viewer applications by using Evil Annotation attacks and in 8 applications using Sneaky Signature by using PDF specification compliant exploits.

We improved both attacks' stealthiness with applications' implementation issues and found only two applications secure to all attacks.

On top, we show how to gain high privileged JavaScript execution in Adobe. We responsibly disclosed these issues and supported the vendors to fix the vulnerabilities.

We also propose concrete countermeasures and improvements to the current specification to fix the issues.

To read more:
https://www.nds.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2021/05/25/Breaking_the_Specification__PDF_Certification.pdf

Number 5

Market entry: Information regarding the authorisation procedure for banks and financial services providers on bafin.de now available in English

BaFin Federal Financial Supervisory Authority

Under “Market entry”, interested parties and applicants can find basic information on the authorisation procedure for the business requiring authorisation, including banking business, investment services, financial services, crypto custody business, payments services, e-money business and hybrid business models.

In the individual sections, BaFin also provides an overview of the applicable key national and European legislation, the various stages of the authorisation procedure and the main assessment criteria.

These sections also provide further information and documents on the submission of applications, such as guidance notices, guidelines, forms and contact details.

The sections offer companies and interested parties an initial guidance so that they can distinguish between the various forms of business requiring authorisation.

They contain information on topics of material importance and on the stages of the authorisation procedure, particularly within the context of the Single Supervisory Mechanism (SSM).

The sections present a summary of the special features of the authorisation procedures for CRR credit institutions, which are conducted by BaFin together with the European Central Bank (ECB) and finally decided by the ECB.

The information on these pages is intended to assist the applicants in establishing which authorisation application is appropriate to their particular business model and enable them to submit a complete and comprehensive application.

The aim is to increase efficiency and enhance the quality of the application procedure in terms of content and correctness while ensuring faster processing times.

BaFin has additionally set up a new ”Passporting“ section which replaces the previous sections “EU/EEA credit institutions” and “EU/EEA investment services enterprises“ and explains the topics of importance in greater detail.

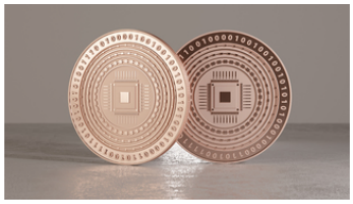
Market entry

Content

- Banking business
- Investment services
- Financial services
- Crypto custody business
- Payment services and e-money business
- Hybrid business models

Crypto custody business

In Germany, the custody, management and protection of crypto assets or private cryptographic keys used to keep, store or transfer cryptoassets – referred to as crypto custody business – is likewise a financial service subject to the authorisation requirement.



Crypto custody business

You can find more information on crypto custody business and the requirements for being granted the necessary authorisation on the overview page regarding › Crypto custody business.

To read more:
https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Markteintritt/markteintritt_node_en.html

Number 6

The Green Swan Conference - Coordinating finance on climate Watch the livestream

The Bank for International Settlements, Bank of France, International Monetary Fund and Network for Greening the Financial System are joining forces to co-sponsor a truly unique global virtual conference on "How in practice can the financial sector take immediate action against climate change-related risks?".

12:15 - 1:15PM / Introduction and opening panel: Why this Conference? How in practice can the financial sector take immediate action against climate change-related risks?

Moderator: Minouche Shafik (LSE)

- Kristalina Georgieva (IMF)
- François Villeroy de Galhau (Banque de France)
- Frank Elderson (ECB; NGFS)
- Agustín Carstens (BIS)

1:15PM - 1:45PM / Special guest speech by Mark Carney (Finance Adviser to the UK Prime Minister for COP 26; UN Special Envoy on Climate Action and Finance)

3:15PM - 3:45PM / Special guest speech by Robert Engle (Michael Armellino Professor of Finance, NYU Stern School of Business)

3:45PM - 4:15PM / Our climate crisis, the financial system and the sustainability revolution

Special guest speech by Al Gore (Chairman, Generation Investment Management)

5:45PM - 6:00PM / Climate risks, financial markets and central banks' risk management

Special guest speech by Jens Weidmann (Chair of the Board, BIS)

6:00PM - 6:30PM / Climate change: our most global challenge

Special guest speech by Tao Zhang (Deputy Managing Director, IMF)

You may visit:
https://www.bis.org/events/green_swan_2021/overview.htm

Number 7

Cyber resilience practices - Executive Summary

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

The financial sector faces significant exposure to cyber risk given that it is information technology-intensive and highly interconnected through payment systems.

Therefore, it is important for financial firms to strengthen their cyber resilience, which is defined by the Financial Stability Board (FSB) as "the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents."

Within the financial sector, banks typically have the most public-facing products and services.

Bank systems have multiple points of contact with outside parties, which can mean significant vulnerability to cyberattacks, with those interfaces being used as entry points for attacks targeting other parts of the financial system.

Bank supervisory authorities have established regulatory and supervisory frameworks to enhance banks' cyber resilience.

Cyber-resilience:

Range of practices

December 2018

In 2018, the Basel Committee on Banking Supervision (BCBS) issued a report entitled *Cyber-resilience: Range of practices* that describes and compares regulatory approaches and supervisory practices across BCBS member jurisdictions. You may visit:
https://www.bis.org/bcbs/publ/d454.pdf

Regulation and supervision

Regulators expect banks to address cyber risk either in their risk management and/or information security frameworks or in their specific cybersecurity strategies.

The latter includes requirements related to governance and oversight; risk ownership and accountability; information security; periodic evaluation and monitoring of cybersecurity controls; incident response; business continuity; and recovery planning.

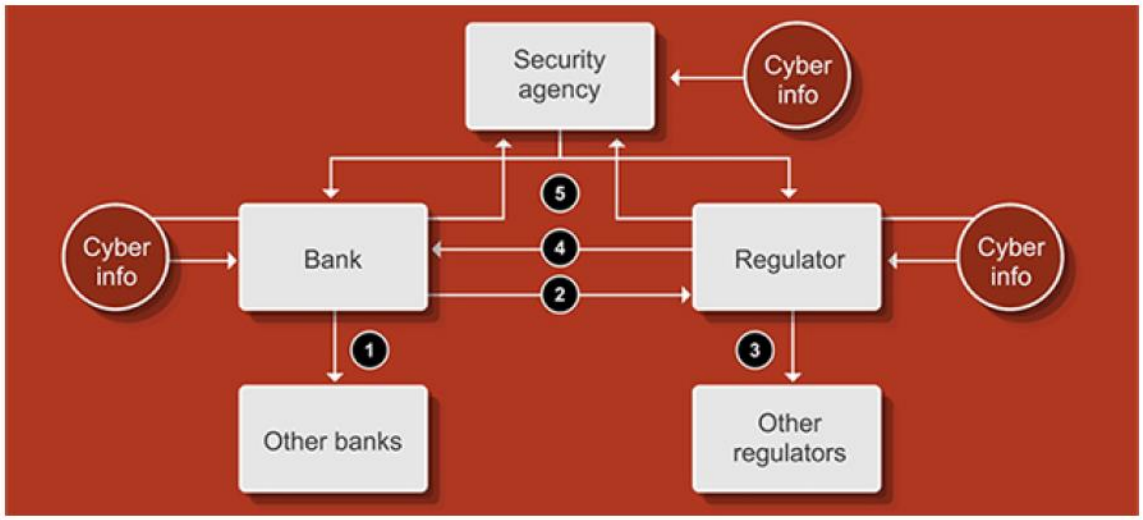
Supervisors assess banks' cybersecurity controls and their monitoring and surveillance of emerging threats. These assessments are based on banks' adherence to existing industry standards.

Supervisory assessments also include challenges to bank approaches to testing controls and the remediation of issues identified.

Challenges can include the review of control testing reports, which may be part of a more formal testing programme.

Such a programme could employ various testing methodologies and practices, such as vulnerability assessment, penetration testing and red team testing.

To read more: https://www.bis.org/fsi/fsisummaries/cyber_resilience.pdf



Number 8

Whom do consumers trust with their data? US survey evidence

Olivier Armantier, Sebastian Doerr, Jon Frost, Andreas Fuster
and Kelly Shue

BIS

Key takeaways

- In a recent survey, US households say they are more likely to trust traditional financial institutions than government agencies or fintechs to safeguard their personal data. They have far less trust in big techs.

- This pattern differs across demographic groups: respondents from racial minorities have less trust in financial institutions, while younger respondents trust fintechs relatively more. Female, minority and younger respondents are more concerned about implications of data-sharing for their personal safety.

- A quarter of respondents say Covid-19 made them less willing to share data. In this group, nearly half became less willing to share with big techs. Concerns centred on identity theft and abuse of data.

- As the economy becomes increasingly digital, and new players expand further into financial services, strong data protection policies will become more important to shield consumers from these harms.

Personal data lie at the heart of the digital economy. Recommendations for online shopping, personalised financial advice or credit increasingly rely on users' digital footprints (Berg et al (2020)).

Large technology companies (big techs) are muscling their way into payments and lending, leveraging the vast amounts of personal data they have collected in other business lines.

The Covid-19 pandemic has accelerated these trends, forcing many employees to work remotely and consumers to shop online (Alfonso et al (2021)).

The resulting increase in online activity makes personal data even more abundant, and more valuable.

Currently, companies often collect and analyse these personal data without consumers' explicit consent or full understanding.

While the analysis of such data can benefit consumers through improved movie recommendations or better targeted online ads, not everybody is equally comfortable with sharing their data.

Rather, this unrestrained collection of personal data represents an unprecedented erosion of consumer privacy, raising important concerns around data abuse and even personal safety – even if the degree of these concerns may vary across different segments of society.

This Bulletin focuses on the willingness of consumers to share data and trust in different actors, based on a representative high-quality survey of US household heads.

It assesses Americans' trust in different counterparties to safely handle their data – governments, traditional financial institutions (FIs), fintechs and large technology firms (big techs) – according to differences in the respondents' gender, ethnicity and age.

The Bulletin also investigates how Covid-19 has changed attitudes and concerns towards privacy. It concludes by discussing the implications for data privacy and digital identity in financial services.

The Survey of Consumer Expectations

We investigate the attitudes towards data privacy of Americans in the Survey of Consumer Expectations (SCE).

The SCE is a high-quality monthly, internet-based survey produced by the Federal Reserve Bank of New York.

Launched in 2013, it is used extensively to help researchers and policymakers understand how expectations are formed and how they affect consumer behaviour.

The SCE is a 12-month rotating panel of roughly 1,300 nationally representative US household heads.

New respondents are drawn each month to match demographic targets from the American Community Survey, and they stay on the panel for up to 12 months before rotating out.

The survey's main aim is to collect expectations for a wide range of economic outcomes (eg inflation, income, spending, household finance, employment and housing).

The survey includes a wealth of detailed demographic information, including the respondent's gender, race, age, income, education, financial literacy and willingness to take risks (Armantier et al (2017)).

To understand how consumers value their data privacy, what determines their willingness to share data and how much they trust different counterparties, the September 2020 survey contained an additional module.

The module asked detailed questions on respondents' attitudes towards data privacy, for example how much they trust different counterparties to safeguard their data, and how the Covid-19 pandemic has affected these attitudes.

In what follows, we use this information to investigate how consumers' attitudes towards and concerns about privacy differ across demographic groups and whether they have changed in response to the pandemic.

To read more: https://www.bis.org/publ/bisbull42.pdf

Number 9

Another Nobelium Cyberattack

Tom Burt, Corporate Vice President, Customer Security & Trust

Microsoft

UPDATE (May 28, 2021, 1pm PT): Our teams have continued to investigate the latest wave of phishing attacks launched by Nobelium.

Based on what we currently know, the security community should feel good about the collective work done to limit the damage done by this wave of attacks.

As we have notified our targeted customers and watched closely for other reports, we are not seeing evidence of any significant number of compromised organizations at this time.

More importantly, antivirus services, like Microsoft Defender Antivirus, and endpoint detection and response products, such as Microsoft Defender for Endpoint, are identifying and protecting against the malware being used in this wave of attacks and are working in combination with Microsoft Defender for Office 365.

It is important for all users to employ basic cybersecurity hygiene, including using multi-factor authentication, using antivirus/antimalware software and being careful not to click on links in email, unless you can confirm reliability to minimize the risk of being phished.

We will continue to monitor the situation.

This week we observed cyberattacks by the threat actor Nobelium targeting government agencies, think tanks, consultants, and non-governmental organizations.

This wave of attacks targeted approximately 3,000 email accounts at more than 150 different organizations.

While organizations in the United States received the largest share of attacks, targeted victims span at least 24 countries.

At least a quarter of the targeted organizations were involved in international development, humanitarian, and human rights work.

Nobelium, originating from Russia, is the same actor behind the attacks on SolarWinds customers in 2020.

These attacks appear to be a continuation of multiple efforts by Nobelium to target government agencies involved in foreign policy as part of intelligence gathering efforts.

Nobelium launched this week's attacks by gaining access to the Constant Contact account of USAID. Constant Contact is a service used for email marketing.

From there, the actor was able to distribute phishing emails that looked authentic but included a link that, when clicked, inserted a malicious file used to distribute a backdoor we call NativeZone.

This backdoor could enable a wide range of activities from stealing data to infecting other computers on a network.

You can read more about the technical aspects of these attacks in this blog post from the Microsoft Threat Intelligence Center (MSTIC).

Many of the attacks targeting our customers were blocked automatically, and Windows Defender is blocking the malware involved in this attack.

We're also in the process of notifying all of our customers who have been targeted.

We detected this attack and identified victims through the ongoing work of the MSTIC team in tracking nation-state actors.

We have no reason to believe these attacks involve any exploit against or vulnerability in Microsoft's products or services.

These attacks are notable for three reasons.

First, when coupled with the attack on SolarWinds, it's clear that part of Nobelium's playbook is to gain access to trusted technology providers and infect their customers.

By piggybacking on software updates and now mass email providers, Nobelium increases the chances of collateral damage in espionage operations and undermines trust in the technology ecosystem.

Second, perhaps unsurprisingly, Nobelium's activities and that of similar actors tend to track with issues of concern to the country from which they

are operating. This time Nobelium targeted many humanitarian and human rights organizations.

At the height of the Covid-19 pandemic, Russian actor Strontium targeted healthcare organizations involved in vaccines.

In 2019, Strontium targeted sporting and anti-doping organizations. And we've previously disclosed activity by Strontium and other actors targeting major elections in the U.S. and elsewhere.

This is yet another example of how cyberattacks have become the tool of choice for a growing number of nation-states to accomplish a wide variety of political objectives, with the focus of these attacks by Nobelium on human rights and humanitarian organizations.

Third, nation-state cyberattacks aren't slowing. We need clear rules governing nation-state conduct in cyberspace and clear expectations of the consequences for violation of those rules.

We must continue to rally around progress made by the Paris Call for Trust and Security in Cyberspace, and more widely adopt the recommendations of the Cybersecurity Tech Accord, and the CyberPeace Institute. But, we need to do more.

Microsoft will continue to work with willing governments and the private sector to advance the cause of digital peace.

To read more:
https://blogs.microsoft.com/on-the-issues/2021/05/27/nobelium-cyberattack-nativezone-solarwinds/

Number 10

Private money and central bank money as payments go digital - an update on CBDCs

Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Consensus by CoinDesk 2021 Conference, Washington DC

Technology is driving dramatic change in the U.S. payments system, which is a vital infrastructure that touches everyone.

The pandemic accelerated the migration to contactless transactions and highlighted the importance of access to safe, timely, and low-cost payments for all.

With technology platforms introducing digital private money into the U.S. payments system, and foreign authorities exploring the potential for *central bank digital currencies (CBDCs)* in cross-border payments, the Federal Reserve is stepping up its research and public engagement on CBDCs.

As Chair Powell discussed last week, an important early step on public engagement is a plan to publish a discussion paper this summer to lay out the Federal Reserve Board's current thinking on digital payments, with a particular focus on the benefits and risks associated with CBDC in the U.S. context.

Sharpening the Focus on CBDCs

Four developments—the growing role of digital private money, the migration to digital payments, plans for the use of foreign CBDCs in cross-border payments, and concerns about financial exclusion—are sharpening the focus on CBDCs.

First, some technology platforms are developing stablecoins for use in payments networks.

A stablecoin is a type of digital asset whose value is tied in some way to traditional stores of value, such as government-issued, or fiat, currencies or gold.

Stablecoins vary widely in the assets they are linked to, the ability of users to redeem the stablecoin claims for the reference assets, whether they allow unhosted wallets, and the extent to which a central issuer is liable for making good on redemption rights.

Unlike central bank fiat currencies, stablecoins do not have legal tender status.

Depending on underlying arrangements, some may expose consumers and businesses to risk.

If widely adopted, stablecoins could serve as the basis of an alternative payments system oriented around new private forms of money.

Given the network externalities associated with achieving scale in payments, there is a risk that the widespread use of private monies for consumer payments could fragment parts of the U.S. payment system in ways that impose burdens and raise costs for households and businesses.

A predominance of private monies may introduce consumer protection and financial stability risks because of their potential volatility and the risk of run-like behavior.

Indeed, the period in the nineteenth century when there was active competition among issuers of private paper banknotes in the United States is now notorious for inefficiency, fraud, and instability in the payments system.

It led to the need for a uniform form of money backed by the national government.

Second, the pandemic accelerated the migration to digital payments. Even before the pandemic, some countries, like Sweden, were seeing a pronounced migration from cash to digital payments.

To the extent that digital payments crowd out the use of cash, this raises questions about how to ensure that consumers retain access to a form of safe central bank money.

In the United States, the pandemic led to an acceleration of the migration to digital payments as well as increased demand for cash.

While the use of cash spiked at certain times, there was a pronounced shift by consumers and businesses to contactless transactions facilitated by electronic payments.

The Federal Reserve remains committed to ensuring that the public has access to safe, reliable, and secure means of payment, including cash.

As part of this commitment, we must explore—and try to anticipate—the extent to which households' and businesses' needs and preferences may migrate further to digital payments over time.

Third, some foreign countries have chosen to develop and, in some cases, deploy their own CBDC.

Although each country will decide whether to issue a CBDC based on its unique domestic conditions, the issuance of a CBDC in one jurisdiction, along with its prominent use in cross-border payments, could have significant effects across the globe.

Given the potential for CBDCs to gain prominence in cross-border payments and the reserve currency role of the dollar, it is vital for the United States to be at the table in the development of cross-border standards.

Finally, the pandemic underscored the importance of access to timely, safe, efficient, and affordable payments for all Americans and the high cost associated with being unbanked and underbanked.

While the large majority of pandemic relief payments moved quickly via direct deposits to bank accounts, it took weeks to distribute relief payments in the form of prepaid debit cards and checks to households who did not have up-to-date bank account information with the Internal Revenue Service.

The challenges of getting relief payments to these households highlighted the benefits of delivering payments more quickly, cheaply, and seamlessly through digital means.

Policy Considerations

In any assessment of a CBDC, it is important to be clear about what benefits a CBDC would offer over and above current and emerging payments options, what costs and risks a CBDC might entail, and how it might affect broader policy objectives.

I will briefly discuss several of the most prominent considerations.

Preserve general access to safe central bank money

Central bank money is important for payment systems because it represents a safe settlement asset, allowing users to exchange central bank liabilities without concern about liquidity and credit risk.

Consumers and businesses don't generally consider whether the money they are using is a liability of the central bank, as with cash, or of a commercial bank, as with bank deposits.

This is largely because the two are seamlessly interchangeable for most purposes owing to the provision of federal deposit insurance and banking supervision, which provide protection for consumers and businesses alike.

It is not obvious that new forms of private money that reference fiat currency, like stablecoins, can carry the same level of protection as bank deposits or fiat currency.

Although various federal and state laws establish protections for users, nonbank issuers of private money are not regulated to the same extent as banks, the value stored in these systems is not insured directly by the Federal Deposit Insurance Corporation, and consumers may be at risk that the issuer will not be able to honor its liabilities.

New forms of private money may introduce counterparty risk into the payments system in new ways that could lead to consumer protection threats or, at large scale, broader financial stability risks.

In contrast, a digital dollar would be a new type of central bank money issued in digital form for use by the general public. By introducing safe central bank money that is accessible to households and businesses in digital payments systems, a CBDC would reduce counterparty risk and the associated consumer protection and financial stability risks.

Improve efficiency

One expected benefit is that a CBDC would reduce or even eliminate operational and financial inefficiencies, or other frictions, in payments, clearing, and settlement.

Today, the speed by which consumers and businesses can access the funds following a payment can vary significantly, up to a few days when relying on certain instruments, such as a check, to a few seconds in a real-time payments system.

Advances in technology, including the use of distributed ledgers and smart contracts, may have the potential to fundamentally change the way in which

payment activities are conducted and the roles of financial intermediaries and infrastructures.

The introduction of a CBDC may provide an important foundation for beneficial innovation and competition in retail payments in the United States.

Most immediately, we are taking a critical step to build a strong foundation with the introduction of the FedNowSM Service, a new instant payments infrastructure that is scheduled to go into production in two years.

The FedNow Service will enable banks of every size and in every community across America to provide safe and efficient instant payment services around the clock, every day of the year.

Through the banks using the service, consumers and businesses will be able to send and receive payments conveniently, such as on a mobile device, and recipients will have full access to funds immediately.

Promote competition and diversity and lower transactions costs

Today, the costs of certain retail payments transactions are high and not always transparent to end users.

Competition among a diversity of payment providers and payment types has the potential to increase the choices available to businesses and consumers, reduce transactions costs, and foster innovation in end-user services, although it could also contribute to fragmentation of the current payments system.

By providing access to a digital form of safe central bank money, a CBDC could provide an important foundation on which private-sector competition could flourish.

Reduce cross-border frictions

Cross-border payments, such as remittances, represent one of the most compelling use cases for digital currencies.

The intermediation chains for cross-border payments are notoriously long, complex, costly, and opaque.

Digitalization, along with a reduction in the number of intermediaries, holds considerable promise to reduce the cost, opacity, and time required for cross-border payments.

While the introduction of CBDCs may be part of the solution, international collaboration on standard setting and protections against illicit activity will be required in order to achieve material improvements in cost, timeliness, and transparency.

We are collaborating with international colleagues through the Bank for International Settlements, Committee on Payments and Market Infrastructures, and the G7 to ensure the U.S. stays abreast of developments related to CBDC abroad.

We are engaging in several international efforts to improve the transparency, timeliness, and cost-effectiveness of cross-border payments. It will be important to be engaged at the outset on the development of any international standards that may apply to CBDCs, given the dollar's important role as a reserve currency.

Complement currency and bank deposits

A guiding principle for any payments innovation is that it should improve upon the existing payments system. Consumers have access to reliable money in the forms of private bank accounts and central bank issued currency, which form the underpinnings of the current retail payments system. The design of any CBDC should complement and not replace currency and bank accounts.

Preserve financial stability and monetary policy transmission

The introduction of a CBDC has the potential to have wide-reaching effects, and there are open questions about how CBDC could affect financial stability and monetary policy transmission.

Some research indicates that the introduction of a CBDC might raise the risk of a flight out of deposits at weak banks in favor of CBDC holdings at moments of financial stress.

Other research indicates that the increase in competition could result in more attractive terms on transactions accounts and an overall increase in banking system deposits.

Banks play a critical role in credit intermediation and monetary policy transmission, as well as in payments.

Thus, the design of any CBDC would need to include safeguards to protect against disintermediation of banks and to preserve monetary policy transmission more broadly.

While it is critical to consider the ways in which a CBDC could introduce risks relative to the current payments system, it may increase resilience relative to a payments system where private money is prominent.

Protect privacy and safeguard financial integrity

The design of any CBDC would need to both safeguard the privacy of households' payments transactions and prevent and trace illicit activity to maintain the integrity of the financial system, which will require the digital verification of identities.

There are a variety of approaches to safeguarding the privacy of payments transactions while also identifying and preventing illicit activity and verifying digital identities.

Addressing these critical objectives will require working across government agencies to assign roles and responsibilities for preventing illicit transactions and clearly establishing how consumer financial data would be protected.

Increase financial inclusion

Today 5.4 percent of American households lack access to bank accounts and the associated payment options they offer, and a further 18.7 percent were underbanked as of 2017.

The lack of access to bank accounts imposes high burdens on these households, whose financial resilience is often fragile.

At the height of the pandemic, the challenges associated with getting relief payments to hard-to-reach households highlighted that it is important for all households to have transactions accounts.

The Federal Reserve's proposals for strengthening the Community Reinvestment Act emphasize the value of banks providing cost-free, low-balance accounts and other banking services targeted to underbanked and unbanked communities.

And a core goal of FedNow is to provide ubiquitous access to an instant payments system via depository institutions.

CBDC may be one part of a broader solution to the challenge of achieving ubiquitous account access.

Depending on the design, CBDC may have the ability to lower transaction costs and increase access to digital payments. In emergencies, CBDC may offer a mechanism for the swift and direct transfer of funds, providing rapid relief to those most in need.

A broader solution to financial inclusion would also need to address any perceived barriers to maintaining a transaction account, along with the need to maintain up-to-date records on active accounts to reach a large segment of the population.

To explore these broader issues, the Federal Reserve is undertaking research on financial inclusion. The Federal Reserve Bank of Atlanta is launching a public–private sector collaboration as a Special Committee on Payments Inclusion to ensure that cash-based and vulnerable populations can safely access and benefit from digital payments.

This work is complemented by a new Federal Reserve Bank of Cleveland initiative to explore the prospects for CBDC to increase financial inclusion. The initiative will identify CBDC design features and delivery approaches focused on expanding access to individuals who do not currently use traditional financial services.

Technology Considerations

Multidisciplinary teams at the Federal Reserve are investigating the technological and policy issues associated with digital innovations in payments, clearing, and settlement, including the benefits and risks associated with a potential U.S. CBDC.

For example, the TechLab group at the Federal Reserve Board is performing hands-on research and experimentation on potential future states of money, payments, and digital currencies.

A second group, the Digital Innovations Policy program, is considering a broad range of policy issues associated with the rise of digital payments, including the potential benefits and risks associated with CBDC.

To deepen our research on the technological design of a CBDC, the Federal Reserve Bank of Boston is partnering with Massachusetts Institute of Technology's (MIT) Digital Currency Initiative on Project Hamilton to build and test a hypothetical digital currency platform using leading edge technology design options.

This work aims to research the feasibility of the core processing of a CBDC, while remaining agnostic about a range of policy decisions.

MIT and the Boston Fed plan to release a white paper next quarter that will document the ability to meet goals on throughput of geographically dispersed transactions with core processing and create an open source license for the code.

Subsequent work will explore how addressing additional requirements, including resiliency, privacy, and anti-money-laundering features, will impact core processing performance and design.

Banking Activities

Research and experimentation are also occurring at supervised banking institutions to explore new technology to enhance their own operations and in response to demands from their clients for services such as custody of digital assets.

While distributed ledger technology may have the potential to improve efficiencies, increase competition, and lower costs, digital assets pose heightened risks such as those related to Bank Secrecy Act/anti-money laundering, cybersecurity, price volatility, privacy, and consumer compliance.

The Federal Reserve is actively monitoring developments in this area, engaging with the industry and other regulators, and working to identify any regulatory, supervisory, and oversight framework gaps.

Given that decisions at one banking agency can have implications for the other agencies, it is important that regulators work together to develop common approaches to ensure that banks are appropriately identifying, monitoring, and managing risks associated with digital assets.

Public Engagement

In light of the growing role of digital private money in the broader migration to digital payments, the potential use of foreign CBDCs in cross-border payments, and the importance of financial inclusion, the Federal Reserve is stepping up its research and public engagement on a digital version of the U.S. dollar.

Members of Congress and executive agencies are similarly exploring this important issue. As noted above, to help inform these efforts, the Federal Reserve plans to issue a discussion paper to solicit public comment on a range of questions related to payments, financial inclusion, data privacy, and information security, with regard to a CBDC in the U.S. context.

The Federal Reserve remains committed to ensuring a safe, inclusive, efficient, and innovative payments system that works for all Americans.

To read more:
https://www.federalreserve.gov/newsevents/speech/brainard20210524a.htm

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.

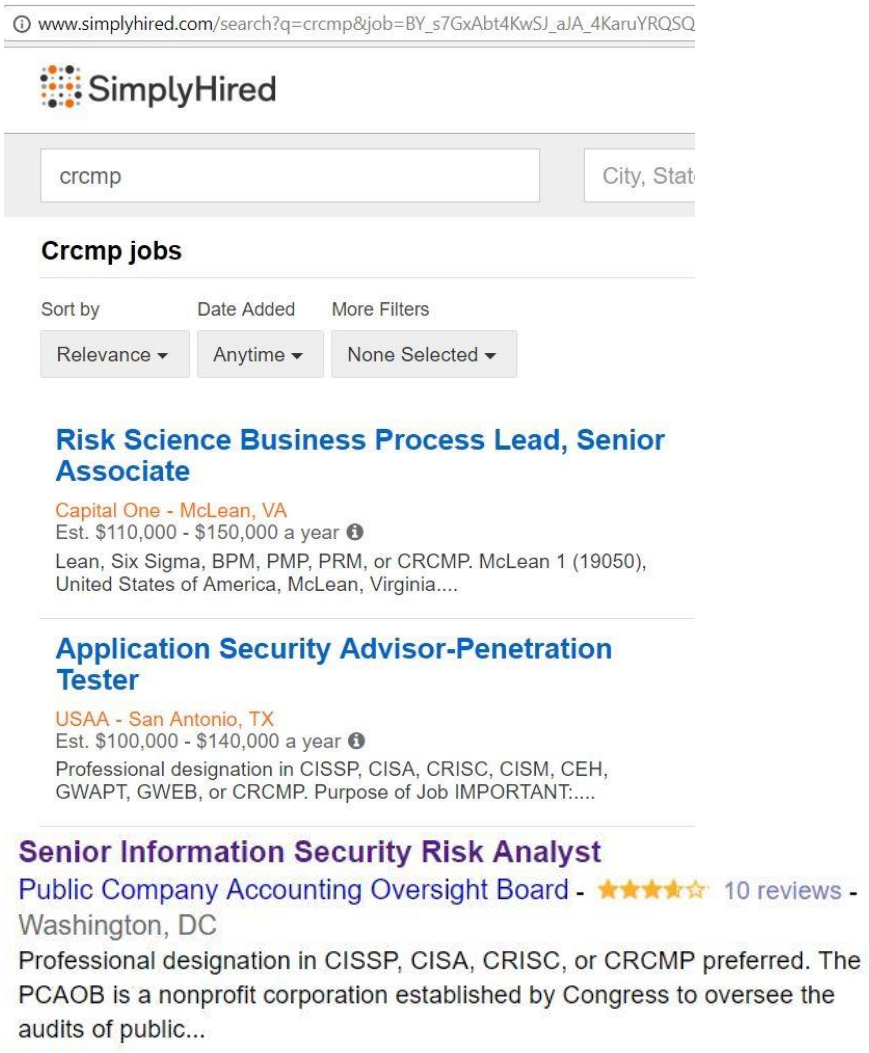
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

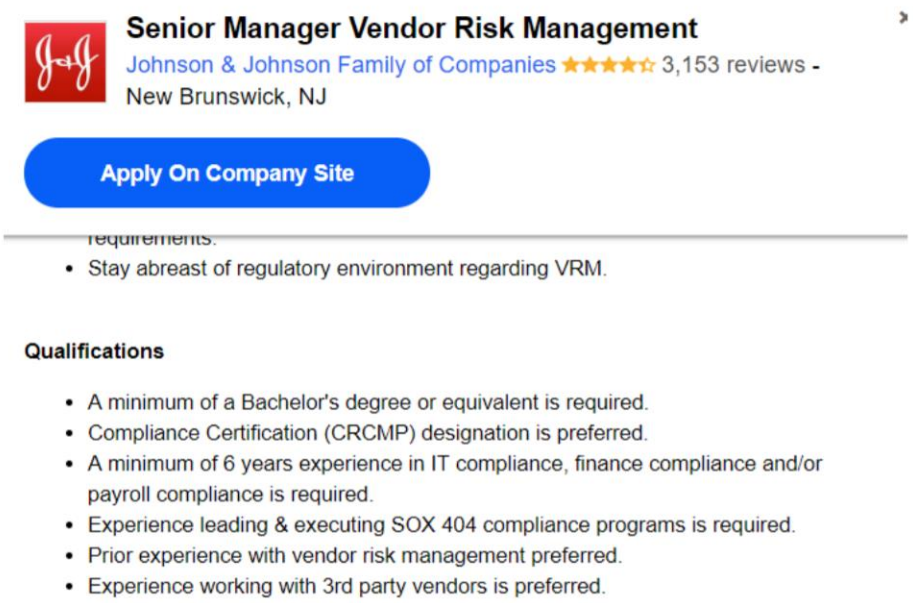
You can explore what we offer to our members:

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.