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

Monday, March 20, 2023

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

Dear members and friends,

I have just read for the second time the new US Cybersecurity Strategy of March 2023. There are some parts in this strategy that are very interesting. We read:

"Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States, including by:

- Strategically employing all tools of national power to disrupt adversaries;

- Engaging the private sector in disruption activities through scalable mechanisms; and,

- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners."

PILLAR TWO | DISRUPT AND DISMANTLE THREAT ACTORS

The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

The phrase "Using all instruments of national power, we will make malicious cyber actors incapable of threatening …" is very interesting, and it is the only way to achieve this objective.

Carl von Clausewitz (a Prussian general, author of "Vom Kriege" (On War), an expert on military strategy) has said: "Pursue one great decisive aim with force and determination."

Isaac Newton believed that "An object in motion tends to remain in motion along a straight line unless acted upon by an outside force". It is time to stop this object in motion, the cyber attacks against our societies, with all instruments of national power in each civilized country, to make malicious cyber actors incapable of threatening us.

Read more at number 1 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 6 (Page 25)

The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks

Number 7 (Page 28)

US Federal Authorities Seize Internet Domain Selling Malware Used to Illegally Control and Steal Data from Victims' Computers

Number 8 (Page 31)

Cyber criminals use Eurovision as the latest phishing lure

Number 9 (Page 33)

DARPA Seeks Input to Advance Hybrid Quantum/Classical Computers

Number 10 (Page 36)

Sanctions and Export Controls Compliance

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls

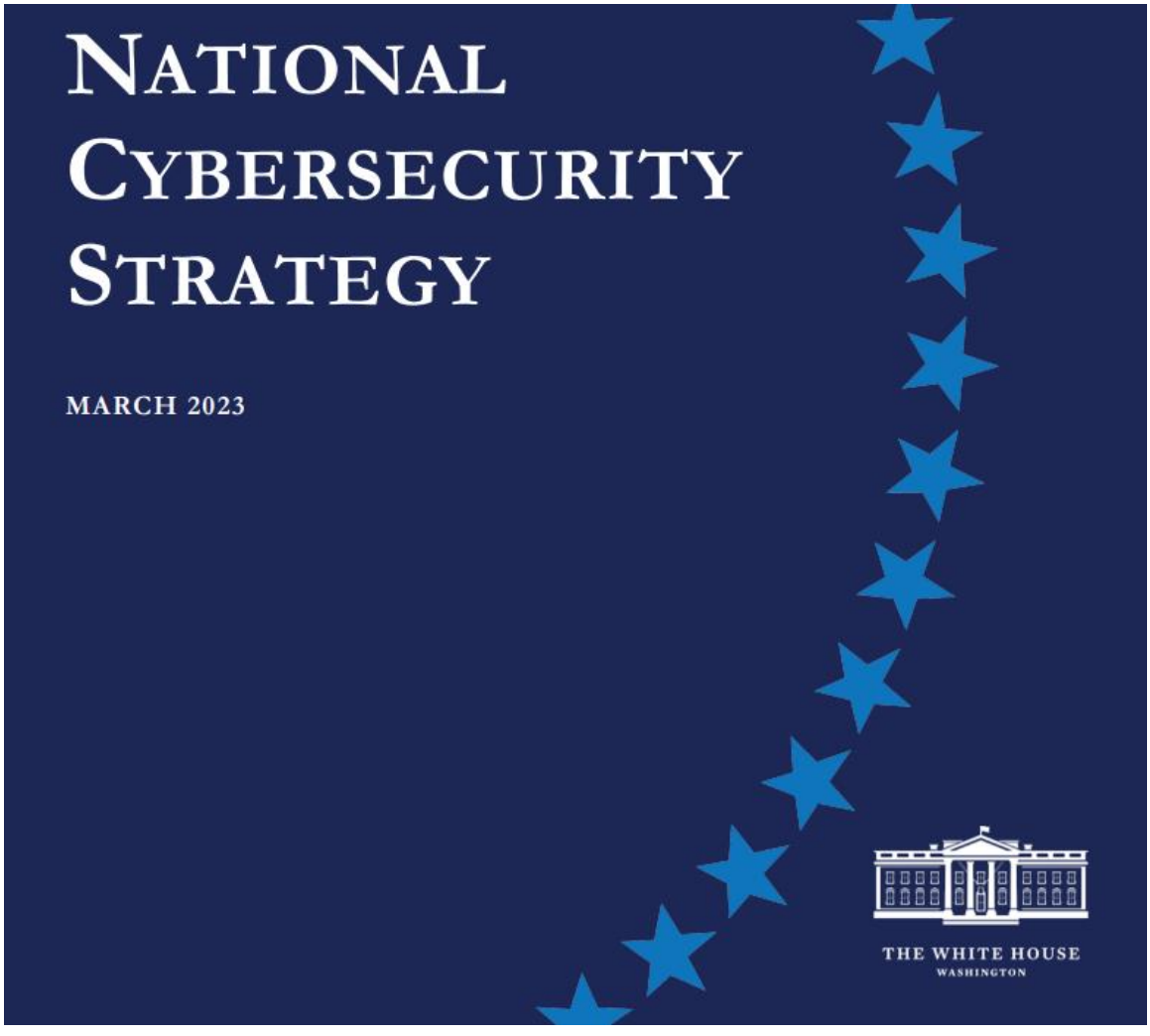
Number 1

The new US National Cybersecurity Strategy

THE WHITE HOUSE

The Biden-Harris Administration released the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans.

In this decisive decade, the United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society. To realize this vision, we must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.



1. We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local

governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.

2. We must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.

The Strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity.

TABLE OF CONTENTS

VISION

Our rapidly evolving world demands a more intentional, more coordinated, and more well-resourced approach to cyber defense. We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests. At the same time, next-generation technologies are reaching maturity at an accelerating pace, creating new pathways for innovation while increasing digital interdependencies.

This Strategy sets out a path to address these threats and secure the promise of our digital future. Its implementation will protect our investments in rebuilding America's infrastructure, developing our clean energy sector, and re-shoring America's technology and manufacturing base. Together with our allies and partners, the United States will make our digital ecosystem:

- **Defensible,** where cyber defense is overwhelmingly easier, cheaper, and more effective;

- **Resilient,** where cyber incidents and errors have little widespread or lasting impact; and,

- **Values-aligned,** where our most cherished values shape—and are in turn reinforced by— our digital world.

The Administration has already taken steps to secure cyberspace and our digital ecosystem, including the National Security Strategy, Executive Order 14028 (Improving the Nation's Cybersecurity), National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems), M-22-09 (Moving the U.S. Government Toward Zero-Trust Cybersecurity Principles), and National Security Memorandum 10 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems). Expanding on these efforts, the Strategy recognizes that cyberspace does not exist for its own end but as a tool to pursue our highest aspirations.

APPROACH

This Strategy seeks to build and enhance collaboration around five pillars:

1. **Defend Critical Infrastructure** – We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides, including by:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance;

- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services; and,

- Defending and modernizing Federal networks and updating Federal incident response policy

2. **Disrupt and Dismantle Threat Actors** – Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States, including by:

- Strategically employing all tools of national power to disrupt adversaries;

- Engaging the private sector in disruption activities through scalable mechanisms; and,

- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners.

PILLAR TWO | DISRUPT AND DISMANTLE THREAT ACTORS

The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

3. **Shape Market Forces to Drive Security and Resilience** – We will place responsibility on those within our digital ecosystem that are best positioned to reduce risk and shift the consequences of poor cybersecurity away from the most vulnerable in order to make our digital ecosystem more trustworthy, including by:

- Promoting privacy and the security of personal data;

- Shifting liability for software products and services to promote secure development practices; and,
- Ensuring that Federal grant programs promote investments in new infrastructure that are secure and resilient.

4. **Invest in a Resilient Future** – Through strategic investments and coordinated, collaborative action, the United States will continue to lead the world in the innovation of secure and resilient next-generation technologies and infrastructure, including by:

- Reducing systemic technical vulnerabilities in the foundation of the Internet and across the digital ecosystem while making it more resilient against transnational digital repression;

- Prioritizing cybersecurity R&D for next-generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure; and,

- Developing a diverse and robust national cyber workforce

5. **Forge International Partnerships to Pursue Shared Goals** – The United States seeks a world where responsible state behavior in cyberspace

is expected and reinforced and where irresponsible behavior is isolating and costly, including by:

- Leveraging international coalitions and partnerships among like-minded nations to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition;

- Increasing the capacity of our partners to defend themselves against cyber threats, both in peacetime and in crisis; and,
- Working with our allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology and operational technology products and services.

Coordinated by the Office of the National Cyber Director, the Administration's implementation of this Strategy is already underway.

To read more:
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Number 2

Basel III Monitoring Report

BIS

Highlights of the Basel III monitoring exercise as of 30 June 2022

- After their record high at end-2021, initial Basel III capital ratios fall to prepandemic levels

- Liquidity ratios decline but remain above pre-pandemic levels

To assess the impact of the Basel III framework on banks, the Basel Committee on Banking Supervision monitors the effects and dynamics of the reforms.

For this purpose, a semiannual monitoring framework has been set up on the risk-based capital ratio, the leverage ratio and the liquidity metrics using data collected by national supervisors on a representative sample of institutions in each country.

Since the end2017 reporting date, the report also captures the effects of the Committee's finalisation of the Basel III reforms.

This report summarises the aggregate results using data as of 30 June 2022. 2 It includes a special feature on Regional distributions of Group 1 and Group 2 banks and their impact on results in the Basel III monitoring reports.

The Committee believes that the information contained in the report will provide relevant stakeholders with a useful benchmark for analysis. Information considered for this report was obtained by voluntary and confidential data submissions from individual banks and their national supervisors.

On the jurisdictional level, there may be mandatory data collections ongoing, which also feed into this report.

Data were included for 181 banks, including 114 large internationally active ("Group 1") banks, among them all 30 G-SIBs and 66 other ("Group 2") banks.

Members' coverage of their banking sector is very high for Group 1 banks, reaching 100% coverage for some countries, while coverage is lower for

Group 2 banks and varies by country. In general, this report does not consider any transitional arrangements such as grandfathering arrangements.

Rather, the estimates presented generally assume full implementation of the Basel III requirements based on data as of 30 June 2022.

No assumptions have been made about banks' profitability or behavioural responses, such as changes in bank capital or balance sheet composition, either since this date or in the future.

Furthermore, the report does not reflect any additional capital requirements under Pillar 2 of the Basel III framework or any higher loss absorbency requirements for domestic systemically important banks, nor does it reflect any countercyclical capital buffer requirements.

Overview of results — Table 1

	31 December 2021[1]			30 June 2022		
	Group 1	Of which: G-SIBs	Group 2	Group 1	Of which: G-SIBs	Group 2
Initial Basel III framework						
CET1 ratio (%)	13.4	13.1	17.7	12.7	12.6	16.9
Target capital shortfalls (€ bn)[2]	0.0	0.0	0.0	0.0	0.0	0.0
TLAC shortfall 2022 minimum (€ bn)	7.5	7.5		35.1	35.1	
Total accounting assets (€ bn)	81,399	56,353	4,414	84,094	61,185	2,459
Leverage ratio (%)[3]	6.6	6.5	6.3	6.0	5.9	5.8
LCR (%)	140.9	138.5	221.9	138.4	137.5	220.1
NSFR (%)	125.1	126.9	134.3	123.5	125.2	132.5
Fully phased-in final Basel III framework (2028)						
Change in Tier 1 MRC at the target level (%)	2.4	2.3	5.7	2.8	3.2	-2.0
CET1 ratio (%)	13.0	12.9	14.4	12.5	12.5	14.5
Target capital shortfalls (€ bn); of which:	0.3	0.3	1.2	7.8	7.8	0.0
CET1	0.0	0.0	0.4	3.5	3.5	0.0
Additional Tier 1	0.0	0.0	0.4	1.9	1.9	0.0
Tier 2	0.3	0.3	0.5	2.4	2.4	0.0
TLAC shortfall 2022 minimum (€ bn)	7.5	7.5		29.8	29.8	
Leverage ratio (%)[3]	6.4	6.3	6.2	6.0	6.0	5.9

See Table A.4 for the target level capital requirements. [1] The values for the previous period may differ slightly from those published in the end-December 2021 report at the time of its release. This is caused by data resubmissions for previous periods to improve the underlying data quality and enlarge the time series sample. [2] Uses the 2017 definition of the leverage ratio exposure measure. [3] The leverage ratios reflect temporary exclusions from leverage exposures introduced in some jurisdictions.

Source: Basel Committee on Banking Supervision.

• Compared with the end-December 2021 reporting period, the average Common Equity Tier 1 (CET1) capital ratio under the initial Basel III framework fell to 12.7% for Group 1 banks.

• The average impact of the final Basel III framework on the Tier 1 Minimum Required Capital (MRC) of Group 1 banks is slightly higher (+2.8%) when compared with the 2.4% increase at end December 2021. The average increase for G-SIBs is 3.2%.

• After reporting an all-time low for capital shortfalls in December 2021, June 2022 shows an increase in capital shortfalls once again, marking the highest value since H1 2020 for Group 1 banks and G-SIBs due to an improvement in data reporting quality.

• Applying the 2022 minimum TLAC requirements and the initial Basel III framework, three of the 25 G-SIBs reporting total loss-absorbing capacity (TLAC) data reported an aggregate incremental shortfall of €35.1 billion when adding back temporary leverage ratio exemptions.

• Group 1 banks' average Liquidity Coverage Ratio (LCR) fell from 140.9% to 138.4% while the average Net Stable Funding Ratio (NSFR) fell from 125.1% to 123.5%.

• Group 2 banks' results based on the unbalanced sample should not be compared with the previous period due to significant changes in the sample.

To read more: https://www.bis.org/bcbs/publ/d546.pdf

Number 3

The quick and the dead - building up cyber resilience in the financial sector

Fabio Panetta, Member of the Executive Board of the European Central Bank, at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main.

The proliferation of cyber threat actors combined with an increase in remote working and greater digital interconnectedness is raising the risk, frequency and severity of cyberattacks.

Increasingly, cyber criminals are launching ransomware attacks and demanding payment in crypto. Cyberattacks related to geopolitical developments – Russia's aggression against Ukraine in particular – have also become a more common feature of the cyber-threat landscape.

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) has played a key role in protecting the security and integrity of the financial system from these threats.

You may visit:
https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ECRB_mandate.pdf

EUROPEAN CENTRAL BANK
EUROSYSTEM

ECB-PUBLIC
26 January 2018

Mandate of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

The last three years have shown that we can work under adverse conditions towards a common goal. Our financial infrastructures have proven their resilience to cyber threats. But this does not mean we can become complacent or any less vigilant in the face of cyber threats. We simply cannot afford to fall behind the curve: cybersecurity must be the backbone of digital finance.

Today I will take stock of the ECRB's work. I will then discuss current cyber threats and emerging risks before outlining the implications for our work in the future.

The contribution of the Euro Cyber Resilience Board

The ECRB brings together private and public stakeholders across pan-European financial infrastructures, critical service providers, central banks and other authorities.

This offers a unique prism through which the ECRB can identify and fix any weaknesses which cyberattacks could potentially exploit in order to propagate, which in turn would cause systemic ripples throughout the European financial ecosystem.

Let me give three examples of why the ECRB is such a useful forum for cooperation.

First, in the area of information sharing, the ECRB's Cyber Information and Intelligence Sharing Initiative (CIISI-EU) allows members to exchange information about cyber threats and mitigation in a secure and trusted group environment.

Second, the ECRB has established a crisis coordination protocol that facilitates cooperation and coordination, allowing members to exchange and respond to major cyber threats and incidents.

Third, in the area of training and awareness, the ECRB conducts joint assessments and training sessions to increase common knowledge and understanding.

A key pillar of the ECB's cyber strategy for financial infrastructures is the TIBER-EU framework for threat-led penetration testing, also known as red teaming. In June 2022 the ECRB organised a dedicated roundtable on TIBER-EU where members shared their experience of these kinds of exercises.

In view of their systemic role in the financial system, we will continue to focus on pan-European financial infrastructures. Nonetheless, financial infrastructures are increasingly interdependent through horizontal and vertical links and common participants.

They are also reliant on information and communication technology and on third-party service providers. As a result, these infrastructures are exposed to common risks and vulnerabilities through which cyberattacks could propagate swiftly if they are not rigorously managed. The ECRB allows us to join forces to address these risks on a sector-wide level.

Adapting to a constantly changing cyber threat landscape

Let me now turn to the cyber threat landscape.

Threats are becoming increasingly complex. Recent attacks call for constant vigilance at an operational level, and the continuous reassessment of regulatory and oversight frameworks to see whether they need to be updated. Significant but unpredictable shifts can occur at any time. We must therefore be prepared to understand them and to adapt quickly in order to mitigate the financial ecosystem's susceptibility to cyberattacks.

The ECRB has identified supply chain attacks and ransomware as key threats in the current environment, and artificial intelligence (AI) as an emerging threat. We have also witnessed how geopolitical developments, most recently Russia's aggression against Ukraine, have weaponised cyberspace. The most prominent examples are distributed denial-of-service (DDoS) attacks against government and financial entities.

Let me discuss the key current and emerging threats in more detail.

Supply chain attacks

The financial ecosystem's reliance on third-party products and services is a key risk, especially when financial entities outsource critical functions to them. An attack on these third parties or on their products and services can disrupt and harm the financial infrastructures that rely on them, with spillovers to interconnected entities.

When such third-party products and services are widely used in the financial ecosystem, a cyberattack can have widespread, possibly systemic effects by having an impact on multiple financial entities at once. That is why cyber threat actors target these third parties. In so doing, they can compromise numerous financial entities simultaneously.

The recent cyberattack on the third-party provider ION Cleared Derivatives shows how an attack on one software provider may cascade onto their clients. In this specific case, the disruptions to the trading and clearing of financial derivatives remained limited, but we cannot ignore scenarios where the attacks could have propagated quickly, disrupting the financial system.

This case signalled the need for financial entities to review their third-party providers, the providers of these third-parties, their cyber resilience levels and the systemic impact that may ensue from a cyberattack on any of these providers.

In particular, it is vital to assess critical service dependencies on third-party products and services which could be disrupted or even terminated as a result of a cyberattack. Mitigating measures need to be put in place.

Against this background, the G7 recently updated its Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector. In addition, the ECRB set up a working group in 2022 to support third-party cyber risk management.

We must have a cyber resilience mindset at all times. The question we must ask is not if a cyberattack will happen, but whether we are ready to respond when it happens.

Over the past year, the ECRB has worked on a conceptual model for how the financial infrastructure ecosystem could manage such a crisis if it occurred. It has also developed protocols and networks aimed at supporting a collective, consistent and comprehensive response to a cyber crisis by stakeholders.

Ransomware

The proliferation of ransomware is one of the most significant challenges currently facing financial entities. Not only may ransomware attacks result in financial loss, they may also severely disrupt operations.

Even after a ransom is paid, there is no guarantee the decryption key will actually work or that the stolen data will not be publicly disclosed or further misused to extort victims' customers, for example.

Ransomware attacks are growing more sophisticated and damaging, which in turn may enable ransomware threat actors to obtain even more resources. 2022 was one of the most active years for ransomware activity.

However, it was also the first year that the majority of victims of ransomware attacks decided not to pay up, which indicates that the approach towards ransomware attacks is changing.

Authorities globally are stepping up their efforts to counter ransomware. For instance, the G7 issued Fundamental Principles on Ransomware Resilience in October 2022.

We need to tackle ransomware attacks from various angles.

First, every firm must be ready to repel ransomware attacks, either through the use of proper cyber hygiene practices or by ensuring that data is backed up regularly and is kept up-to-date and tamper-proof.

Second, enforcement agencies need to conduct forensic analyses, locate attackers and join forces to prosecute them.

Third, crypto-assets – especially unbacked crypto-assets, which are used to make ransomware payments owing to the anonymity and money laundering possibilities they offer – need to be strictly regulated. Similarly, crypto-asset transfers must be traceable.

The proposed EU Regulation for Markets in Crypto-Assets (MiCA) and revision to the Regulation on information accompanying transfers of funds, which extends the "travel rule" to crypto-assets, are important steps. However, to be effective and prevent regulatory arbitrage, regulation must be stepped up globally.

Implementation of the Financial Action Task Force (FATF) guidance for crypto-assets and its enforcement at international level are therefore crucial.

In addition, all firms need to have the highest level of cyber controls in place to prevent attacks from being successful and to detect and recover from ransomware attacks.

Moreover, insurance firms can lend their support by obtaining assurances from their clients that they have high-level cyber resilience plans in place before providing cyber risk insurance policies, thus ensuring that these very same policies do not lower firms' incentives to prepare for cyberattacks.

Artificial Intelligence (AI)

Even if we do not realise it, the use of artificial intelligence (AI) is already widespread. We use AI every day, including on our phones, in our homes and at the workplace. And firms use it to harness big data.

AI can help to strengthen cybersecurity, for instance, by improving the detection of highly sophisticated cyberattacks through its ability to identify abnormal system behaviour compared with an established baseline. This is the kind of potential that we need to leverage.

But AI can also multiply cyber risks by, for instance, helping malicious individuals, even those who have limited or no technical skills, draft very convincing phishing emails or identify topics that will achieve the maximum engagement from those being targeted.

To make matters worse, AI can even create and fix code that can be used to exploit and compromise the endpoint.

This opens up new possibilities for malicious individuals to use AI to launch cyberattacks. Although AI development firms try to install safeguards to prevent its unethical use, they can be circumvented.

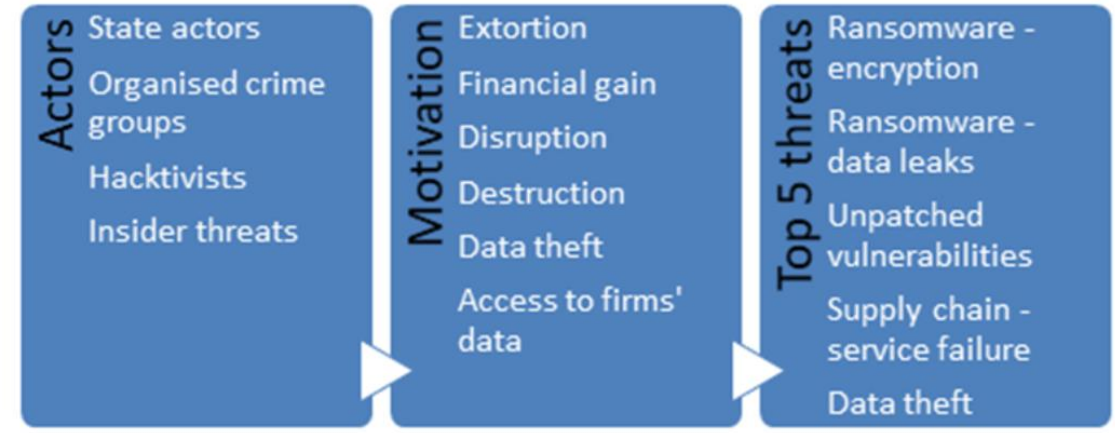
The risks from AI need to be clearly understood and addressed through regulation and oversight.

By exchanging information among its members and organising roundtables and training, the ECRB is in a strong position to raise awareness of risks at an early stage and accumulate knowledge of these types of threats.

For its part, the European Commission has proposed a Regulation on artificial intelligence that aims to address some of the key risks associated with AI.

Chart 1

Cyber threat landscape for financial market infrastructures in Europe



Note: Threats are arranged in descending order of estimated severity.

To read more:
https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230308~92211cd1f5.en.html

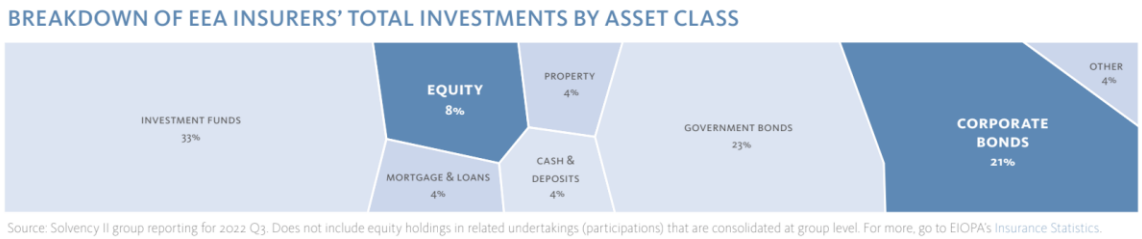
Number 4

Insurers green investments

European Insurance and Occupational Pensions Authority

To meet the EU's climate targets and help speed up society's transition to a net-zero economy, investments in sustainable activities are needed. As long-term investors with an overall balance sheet of around €8 trillion, insurers in the European Economic Area (EEA) can play a significant role in putting our economies on a more sustainable track.

Based on the EU Taxonomy of sustainable activities and using the NACE classification framework, EIOPA analyzed how much of EEA insurers' investments can be considered environmentally sustainable at present.



To read more:
https://www.eiopa.europa.eu/system/files/2023-02/Factsheet%20-%20Green%20investments%202023v5.pdf

Number 5

Looking through a glass onion - lessons from the 2022 Liability Driven Investment (LDI) intervention

Andrew Hauser, Executive Director for Markets of the Bank of England, at the Chicago Booth Initiative on Global Markets' Workshop on Market Dysfunction, University of Chicago Booth School of Business, Chicago, Illinois.

Introduction

It was just over two years ago when Lorie Logan and I first sat down to map out a plan for a working group of the Bank for International Settlements (BIS) Markets Committee on tools for market dysfunction.

A year earlier, central banks around the globe had been required to intervene, at pace and scale, to prevent the sudden 'dash for cash' that followed the announcement of Covid lockdowns from undermining monetary and financial stability.

Those interventions worked, aided by the fact that the stance required to tackle market dysfunction was directionally aligned with that required to achieve monetary policy goals more broadly.

Nevertheless, given the speed with which dysfunction appeared, many central banks had to innovate, using tools they had to hand, rather than those designed specifically for the purpose.

If the mayhem in financial markets in Spring 2020 had been a genuine one-off, that might have been the end of things.

But what Lorie and I wanted to highlight was that, while Covid itself may have been truly exceptional, the financial market propagation mechanisms that turned that shock into a nascent systemic liquidity crisis reflected more structural trends: an increasing reliance by the real economy on core capital markets rather than banks; constraints on market intermediation capacity; and a range of unresolved vulnerabilities in non-bank firms that played an ever-growing role in those markets. In short, even if nothing as awful as Covid ever happened again, market dysfunction at a scale capable of

threatening systemic stability could recur – and in all likelihood, would do so. And central banks needed to be ready to play their part.

Our working group did not seek to provide a single definitive 'playbook' for such events – the range of potential shocks, and different national market and institutional structures, made that impossible. But it did set out a framework of principles and possible tool choices.

And that framework proved invaluable at the Bank of England when, late last year, vulnerabilities in Liability Driven Investment (LDI) funds amplified the impact of an abrupt change in fiscal stance into a self-reinforcing spiral in government bond prices.

Long maturity nominal gilt yields rose by 130 basis points in a matter of days – three times the size of any comparable historical move – and we were required to intervene to safeguard financial stability.

A temporary and targeted backstop purchase facility for gilts proved effective in ending the firesale dynamic, providing the LDI funds with a window to increase their resilience while minimising risks to public funds, market incentives and the stance of monetary policy – which, unlike in 2020, was now in a tightening phase.

In my remarks today, I want to discuss four main lessons that I take from those events:

1. **The changing nature of systemic liquidity risk:** though focus naturally alights on the idiosyncrasies of the autumn fiscal announcements and the UK LDI sector, the real import lies in the features the events had in common with the dash for cash and other similar developments: another reminder, if more were needed, that we face a new era of liquidity risk, originating outside the banking system, that can amplify shocks, destabilise core markets and undermine monetary and financial stability.

2. **Public backstops vs private self insurance:** as a central bank it fell to us to provide a public backstop to prevent systemic liquidity risk from undermining monetary and financial stability. At the same time, the events revealed material weaknesses in pension fund and LDI risk management. Given the costs involved, we must ensure public backstops do not end up substituting for a failure to achieve the appropriate level of private insurance against liquidity risk here and elsewhere in the non-bank sector.

3. **Ensuring we have central bank tools that are effective:** to backstop these new forms of systemic liquidity risk effectively, central banks need the right tools – to detect risks in a timely way; and to respond.

In the LDI case, early warning required the use of qualitative as well as quantitative market intelligence. Effective response required the use of a buy/sell facility. Lending directly to non-banks would not have worked in this case. But it has many desirable properties for other scenarios, and is a high priority for future work.

4. **Calibrating central bank tools to minimise risk:** backstop facilities must be carefully designed if they are to be effective in removing the threat to systemic stability while minimising risks to the stance of monetary policy, to public funds, and to the incentives of market participants. In the LDI case, we sought to achieve that by grounding the objectives of the tool in restoring financial stability, targeting it on the parts of the market most in need of assistance, pricing it as a backstop to ensure we bought no more than needed, and ensuring it was strictly time limited, in its operation and in its unwind.

The LDI operations were successful, but highlight many questions for the future. For me, three in particular stand out:

- Where do societies want to draw the line between public and private insurance against systemic liquidity in non-banks, and how do they ensure regulatory and central bank facility thinking develops in a co-ordinated way?

- What is the right mix of central bank tools between buy/sell and lending/repo facilities? Where lending is preferred, which firms do we need to reach to maintain stability; how do ensure we can reach them (legally and operationally); and what terms and conditions should they face?

- What are the pros and cons of establishing standing facilities, whose terms and conditions are known in advance; versus simply ensuring we are ready to act in a more discretionary ways as/when required?

Like the Beatles' 'glass onion' in my title,footnote[4] these lessons are not meant to be complex or novel.

They bear a wholly intentional family resemblance to the Bagehot principle: a recognition that liquidity risk (in this case, arising in capital markets rather than banks) may threaten system-wide stability; that central banks may have an important role to play in providing a public backstop at scale; but they should do so on terms that minimise risks to public money and complement, rather than substitute for, market incentives. And they draw heavily on a literature on the Market Maker or Last Resort (MMLR) dating back at least to the start of the Global Financial Crisis.

As others have noted, despite this extended history, progress towards institutionalising these insights has been uneven. I hope that the BIS work, coupled with our sadly growing set of live case studies, can help accelerate that process.

Let me elaborate a little on each of my four lessons.

To read more:
https://www.bankofengland.co.uk/speech/2023/march/andrew-hauser-opening-remarks-at-university-of-chicago-booth-school-of-business-workshop

Number 6

The Criminal Division's Pilot Program Regarding Compensation Incentives and Clawbacks

The Department of Justice (Department) is committed to tackling corporate crime and will continue to investigate and prosecute companies (and responsible individuals) who engage in such misconduct.

But the Department's ultimate goal is to prevent corporate crime before it occurs. Through its policies and enforcement actions, the Department strives to deter criminal conduct, incentivize the development and implementation of effective compliance programs, and promote ethical corporate cultures.

Compensation systems that use affirmative metrics and benchmarks can reward compliancepromoting behavior.

Compensation systems that clearly and effectively impose financial penalties for misconduct can also deter risky behavior and foster a culture of compliance.

Consistent with the Deputy Attorney General's September 15, 2022 memorandum setting forth revisions to the Department's corporate criminal enforcement policies, the Department's Criminal Division (Division) has considered how to reward corporations that develop solutions to incentivize better compliance through their compensation systems, including the use of clawback policies.

Throughout this process, one consideration has been how policies may seek to potentially shift the burden of corporate financial penalties away from shareholders—who in many cases do not have a role in misconduct—onto those more directly responsible.

In this review, the Division has consulted with its agency partners, members of the defense bar, academics, experts on executive compensation, and other regulators to gain valuable perspectives and data points.

Accordingly, the Division is conducting a Compensation Incentives and Clawbacks Pilot Program (Program).

As set forth below, the Program provides that, when entering into criminal resolutions, companies will be required to implement compliance-related criteria in their compensation and bonus system and to report to the Division about such implementation during the term of such resolutions.

The Program also directs Division prosecutors to consider possible fine reductions where companies seek to recoup compensation from culpable employees and others who both:

(a) had supervisory authority over the employee(s) or business area engaged in the misconduct and

(b) knew of, or were willfully blind to, the misconduct.

The Program is a three-year initiative applicable to all corporate matters handled by the Division and is effective March 15, 2023.

This Program does not modify the Criminal Division's Corporate Enforcement Policy, the Evaluation of Corporate Compliance Programs, or the Principles of Federal Prosecution of Business Organizations.

At the end of this pilot period, the Division will determine whether the Program will be extended in duration or modified in any respect.

I. Compliance Enhancements

During the Program, every corporate resolution entered into by the Division shall include a requirement that the resolving company implement criteria related to compliance in its compensation and bonus system.

The company must also report to the Division annually during the term of the resolution about its implementation of such criteria.

These criteria may include, but are not limited to:

(1) a prohibition on bonuses for employees who do not satisfy compliance performance requirements;

(2) disciplinary measures for employees who violate applicable law and others who both

(a) had supervisory authority over the employee(s) or business area engaged in the misconduct and

(b) knew of, or were willfully blind to, the misconduct; and

(3) incentives for employees who demonstrate full commitment to compliance processes.

Division prosecutors will use their discretion in fashioning the appropriate requirements based on the particular facts and circumstances of the case, including, but not limited to, applicable foreign and domestic law.

In making this determination, prosecutors will be mindful of, and afford due consideration to, how the company has structured its existing compensation program.

To read more:
https://www.justice.gov/opa/speech/file/1571906/download

Number 7

US Federal Authorities Seize Internet Domain Selling Malware Used to Illegally Control and Steal Data from Victims' Computers

United States Attorney's Office
Central District of California

As part of an international law enforcement effort, federal authorities in Los Angeles this week seized an internet domain that was used to sell computer malware used by cybercriminals to take control of infected computers and steal a wide array of information.

A seizure warrant approved by a United States Magistrate Judge on March 3 and executed on Tuesday led to the seizure of www.worldwiredlabs.com, which offered the NetWire remote access trojan (RAT), a sophisticated program capable of targeting and infecting every major computer operating system.

"A RAT is a type of malware that allows for covert surveillance, allowing a 'backdoor' for administrative control and unfettered and unauthorized remote access to a victim's computer, without the victim's knowledge or permission," according to court documents filed in Los Angeles.

As part of this week's law enforcement action, authorities in Croatia on Tuesday arrested a Croatian national who allegedly was the administrator of the website.

This defendant will be prosecuted by Croatian authorities. Additionally, law enforcement in Switzerland on Tuesday seized the computer server hosting the NetWire RAT infrastructure.

The FBI in Los Angeles in 2020 opened an investigation into worldwidelabs, the only known online distributor of NetWire.

Undercover investigators with the FBI created an account on the website, paid for a subscription plan, and "constructed a customized instance of the NetWire RAT using the product's Builder Tool," according to the affidavit in support of the seizure warrant.

While the website marketed NetWire as a legitimate business tool to maintain computer infrastructure, the affidavit states that NetWire is a malware used for malicious purposes, the software was advertised on hacking forums, and numerous cyber security companies and government agencies have documented instances of the NetWire RAT being used in criminal activity.

"Today's action is a testament to the innovation and flexibility necessary to fighting cybercriminals who operate without borders," said United States Attorney Martin Estrada.

"Our office will continue to forge international alliances to protect our communities from cyber threats. Criminals used NetWire on a global scale, and we have responded by dismantling the infrastructure that has caused untold harm to victims around the world."

"By removing the Netwire RAT, the FBI has impacted the criminal cyber ecosystem," said Donald Alway, the Assistant Director in Charge of the FBI's Los Angeles Field Office.

"The global partnership that led to the arrest in Croatia also removed a popular tool used to hijack computers in order to perpetuate global fraud, data breaches and network intrusions by threat groups and cyber criminals."

This matter is the result of the United States' strong law enforcement cooperation with Croatia and other global partners. The FBI's Los Angeles Field Office; the Croatia Ministry of the Interior, Criminal Police Directorate; Zurich Cantonal Police in Switzerland; the Europol European Cybercrime Center; and the Australian Federal Police conducted the investigation in this matter.

Assistant United States Attorneys Lisa Feldman of the Cyber and Intellectual Property Crimes Section and Maxwell Coll of the Asset Forfeiture and Recovery Section obtained the seizure warrant for the internet domain.

The Office of International Affairs in the Justice Department's Criminal Division provided substantial assistance during the investigation.

To read more:
https://www.justice.gov/usao-cdca/pr/federal-authorities-seize-internet-domain-selling-malware-used-illegally-control-and

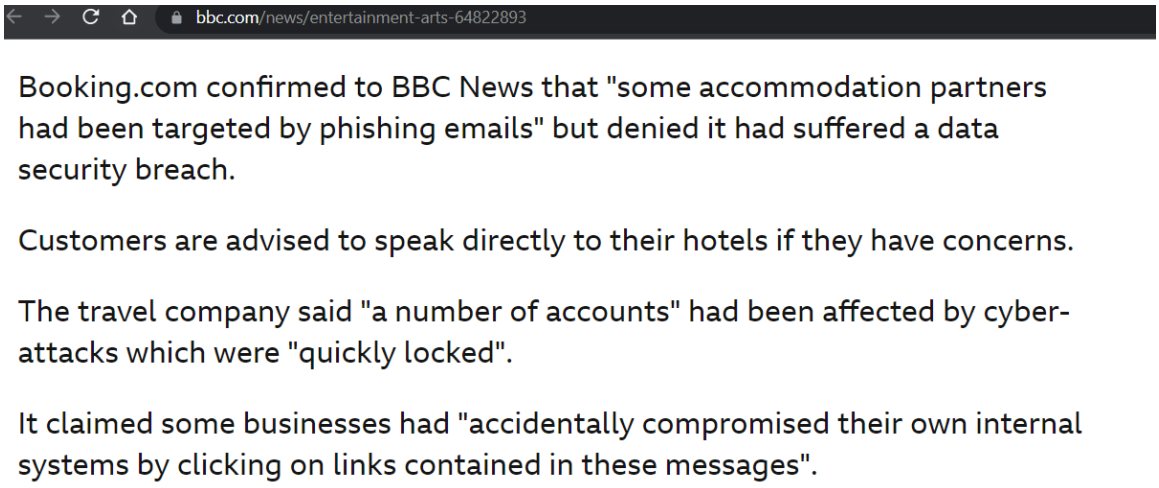
Number 8

Cyber criminals use Eurovision as the latest phishing lure

National Cyber Security Centre

Cyber criminals are targeting hotels hosting people travelling to Liverpool for the Eurovision song contest event in May.

The online travel agent booking.com has confirmed to the BBC they have seen evidence of "some accommodation partners being targeted by phishing emails."


bbc.com/news/entertainment-arts-64822893

Booking.com confirmed to BBC News that "some accommodation partners had been targeted by phishing emails" but denied it had suffered a data security breach.

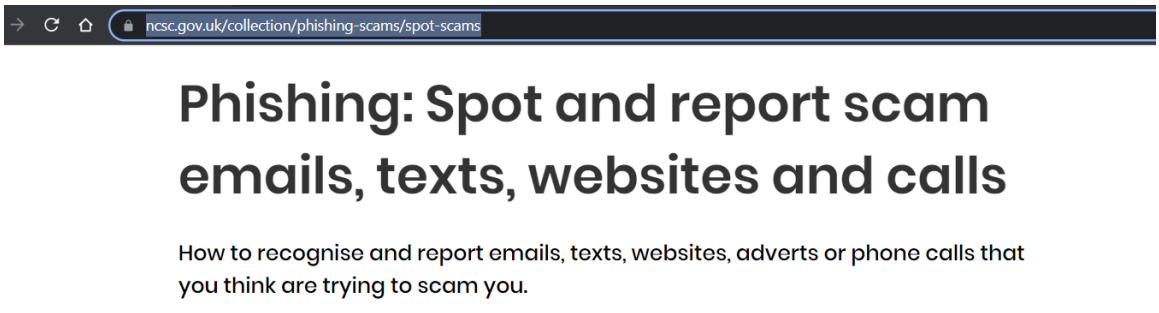
Customers are advised to speak directly to their hotels if they have concerns.

The travel company said "a number of accounts" had been affected by cyber-attacks which were "quickly locked".

It claimed some businesses had "accidentally compromised their own internal systems by clicking on links contained in these messages".

Cyber criminals often take advantage of news and topical events to scam customers.

There are some good ways you can prepare yourself and spot potential scams on the NCSC website, as well as guidance on what to do next if you are a victim of phishing. You may visit:
https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams


ncsc.gov.uk/collection/phishing-scams/spot-scams

Phishing: Spot and report scam emails, texts, websites and calls

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

Cyber criminals may contact you via email, text, phone call or via social media. They will often pretend to be someone (or an organisation) you trust.

If you've been tricked into sharing personal information with a scammer, you can take immediate steps to protect yourself.

Situation	Action
You've provided your banking details	Contact your bank and let them know.
You think your account has already been hacked	You may have received messages sent from your account that you don't recognise, or you may have been locked out of your account, refer to our guidance on recovering a hacked account.
You received the message on a work laptop or phone	Contact your IT department and let them know.
You opened a link on your computer, or followed instructions to install software	Open your antivirus (AV) software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds.
You've given out your password	You should change the passwords on any of your accounts which use the same password.
You've lost money	Tell your bank and report it as a crime to Action Fraud (for England, Wales and Northern Ireland) or Police Scotland (for Scotland).

To read more:
https://www.ncsc.gov.uk/report/threat-report-10th-march-2023

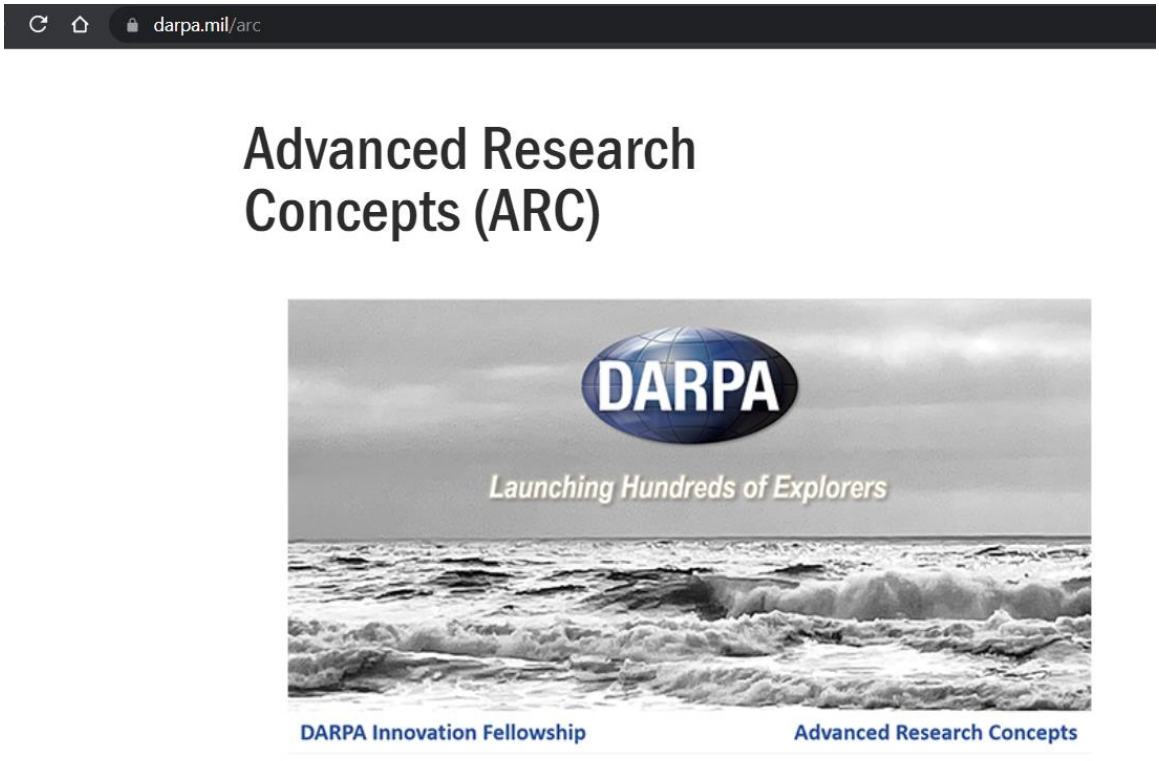
Number 9

DARPA Seeks Input to Advance Hybrid Quantum/Classical Computers

Although fault-tolerant quantum computers are projected to be years to decades away, processors made from tens to hundreds of quantum bits have made significant progress in recent years, especially when working in tandem with a classical computer.

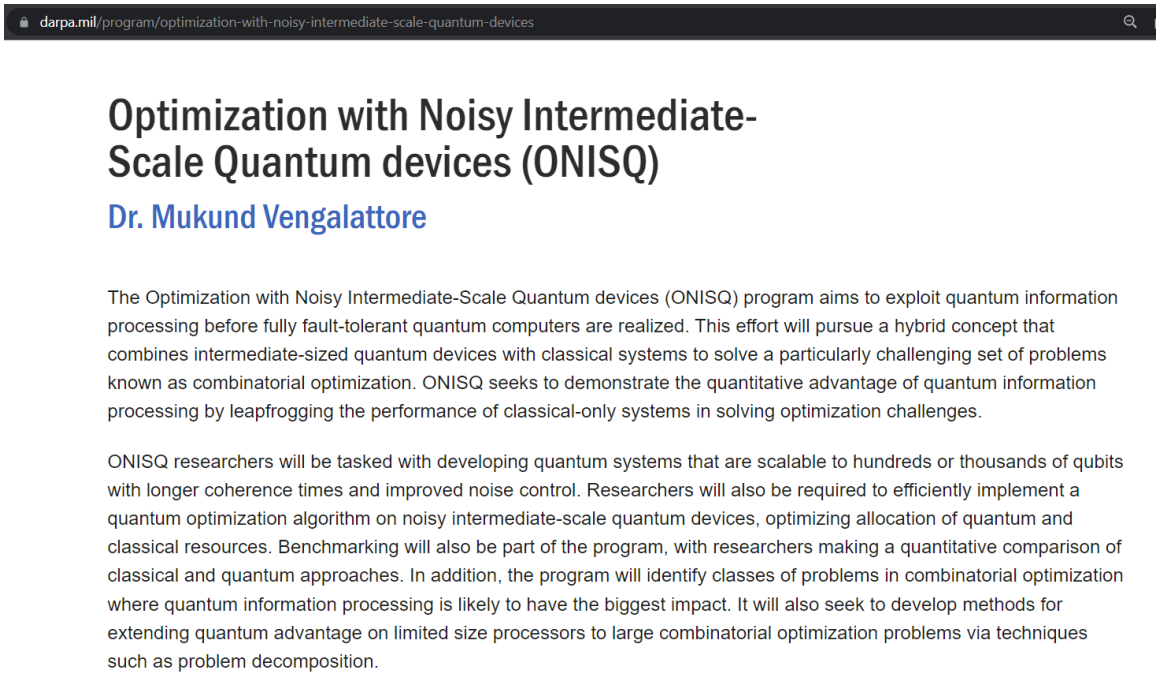
These hybrid quantum/classical systems could enable technical disruption soon by superseding the best classical-only supercomputers in solving difficult optimization challenges and related problems of interest to defense, security, and industry.

DARPA is sponsoring a live webinar on Tuesday, April 11, 2023, to highlight an Advanced Research Concept (ARC) topic called Imagining Practical Applications for a Quantum Tomorrow (IMPAQT).



Registrants will have the opportunity to hear from government experts, university professors, and industry-leading quantum hardware providers as well as participate in live question-and-answer sessions.

"We're billing the webinar as a help day for quantum algorithmists," said DARPA Innovation Fellow Alex Place, who is leading the event. "Building on successes of DARPA's ONISQ (Optimization with Noisy Intermediate-Scale Quantum devices) program, the webinar's goal is to spark innovative ideas and discuss new concepts for making near-term intermediate scale quantum computers, as well as sought-after fault tolerant processors, practical and useful for solving real problems. We're encouraging teams from academia and industry who have expertise in quantum algorithms or a practical problem that could be mapped to a quantum processor to engage with IMPAQT."



IMPAQT is the first of many anticipated DARPA ARC topics. The ARC initiative is designed to speed the pace of innovation by rapidly exploring and analyzing a high volume of promising new ideas.

For more information about ARC, to view the open IMPAQT solicitation, and to see new topics as they become available, visit www.darpa.mil/arc.

The ARC topics are managed by DARPA's innovation fellows, who include recent Ph.D. graduates (within five years of receiving a doctorate) and active-duty military with STEM degrees.

To learn more about the DARPA Innovation Fellowship, current fellows, and how you can apply to become a fellow visit:
www.darpa.mil/innovationfellowship

To read more: https://www.darpa.mil/news-events/2023-03-07

Number 10

Sanctions and Export Controls Compliance

Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note

Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls

Over the year following Russia's illegal and unprovoked war against Ukraine, the U.S. government has used its economic tools to degrade Russia's economy and war machine.

Along with international partners and allies, the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Commerce's Bureau of Industry and Security (BIS) have imposed sanctions and export controls of an unprecedented scope and scale in an effort to degrade Russia's ability to wage its unjust war and to prevent it from taking military action elsewhere.

The Department of Justice (DOJ) has matched these unprecedented restrictions with equally unprecedented enforcement efforts to aggressively prosecute those who violate U.S. sanctions and export control laws, led by the work of Task Force KleptoCapture.

Despite these efforts, malign actors continue to try to evade Russia-related sanctions and export controls.

One of the most common tactics is the use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially Designated Nationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users.

This Note highlights several of these tactics to assist the private sector in identifying warning signs and implementing appropriate compliance measures.

DETECTING SANCTIONS AND EXPORT CONTROL EVASION

It is critical that financial institutions and other entities conducting business with U.S. persons or within the United States, or businesses

dealing in U.S.-origin goods or services or in foreignorigin goods otherwise subject to U.S. export laws, be vigilant against efforts by individuals or entities to evade sanctions and export control laws.

Effective compliance programs employ a risk-based approach to sanctions and export controls compliance by developing, implementing, and routinely updating a compliance program, depending on an organization's size and sophistication, products and services, customers and counterparties, and geographic locations.

Companies such as manufacturers, distributors, resellers, and freight forwarders are often in the best position to determine whether a particular dealing, transaction, or activity is consistent with industry norms and practices, and they should exercise heightened caution and conduct additional due diligence if they detect warning signs of potential sanctions or export violations.

Equally important is the maintenance of effective, risk-based compliance programs that entities can adopt to minimize the risk of evasion. These compliance programs should include management commitment (including through appropriate compensation incentives), risk assessment, internal controls, testing, auditing, and training.

These efforts empower staff to identify and report potential violations of U.S. sanctions and export controls to compliance personnel such that companies can make timely voluntary disclosures to the U.S. government.

Optimally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries.

Common red flags can indicate that a third-party intermediary may be engaged in efforts to evade sanctions or export controls, including the following:

1. Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions;

2. A customer's reluctance to share information about the end use of a product, including reluctance to complete an end-user form;

3. Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;

4. Declining customary installation, training, or maintenance of the purchased item(s);

5. IP addresses that do not correspond to a customer's reported location data;

6. Last-minute changes to shipping instructions that appear contrary to customer history or business practices;

7. Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;

8. Use of personal email accounts instead of company email addresses;

9. Operation of complex and/or international businesses using residential addresses or addresses common to multiple closely-held corporate entities;

10. Changes to standard letters of engagement that obscure the ultimate customer;

11. Transactions involving a change in shipments or payments that were previously scheduled for Russia or Belarus;

12. Transactions involving entities with little or no web presence; or

13. Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus. Such locations may include China (including Hong Kong and Macau) and jurisdictions close to Russia, including Armenia, Turkey, and Uzbekistan.

Further, entities that use complex sales and distribution models may hinder a company's visibility into the ultimate end-users of its technology, services, or products.

To rear more:
https://home.treasury.gov/system/files/126/20230302_compliance_note.pdf

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

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

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

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

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

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

3. *Training and Certification* – Become:

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

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

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

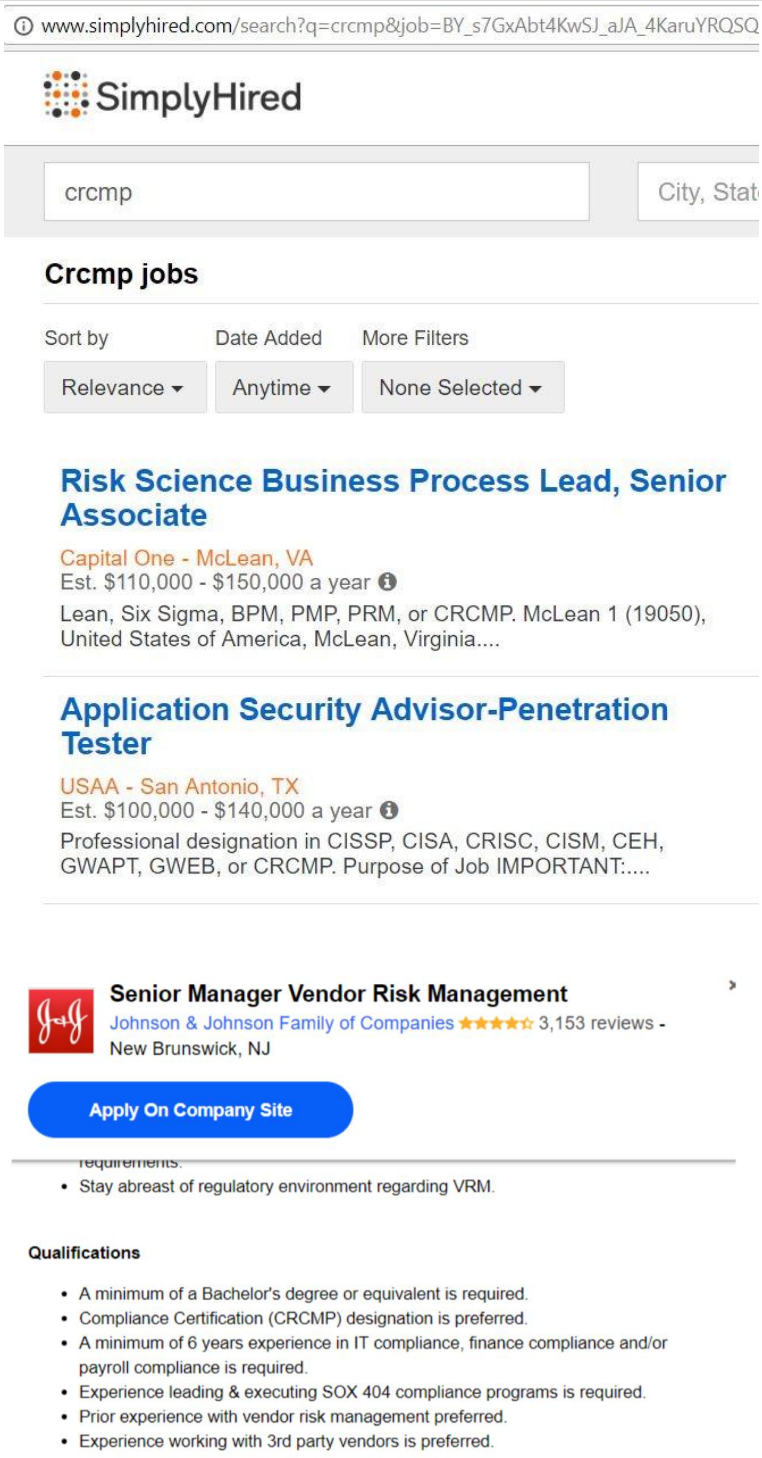
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

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

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

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



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

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

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

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

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

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

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

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

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