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 6, 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,

Confucius believed that "it is easy to hate, and it is difficult to love. All good things are difficult to achieve, and bad things are very easy to get."

The compliance objectives in the EU these days are so difficult to achieve, and so difficult to love. Europe is running out of qualified compliance officers in certain difficult areas:

1. The Digital Services Act entered into force the 17th of February, 2024. In the context of the Russian military invasion in Ukraine, and the particular impact on the manipulation of online information, the Digital Services Act introduces a crisis response mechanism. This mechanism will make it possible to analyse the impact of the activities of very large online platforms (VLOPs) and very large online search engines (VLOSEs).

The Digital Services Act is the most important and most ambitious regulation in the world in the field of the protection of the digital space against the spread of illegal content. There is no other legislative act in the world having this level of ambition to regulate social media, online marketplaces, very large online platforms (VLOPs) and very large online search engines (VLOSEs).

After the Digital Services Act, platforms will not only have to be more transparent, but will also be held accountable for their role in disseminating illegal and harmful content.

Amongst other things, the DSA:

a. Lays down special obligations for online marketplaces in order to combat the online sale of illegal products and services;

b. Introduces measures to counter illegal content online and obligations for platforms to react quickly, while respecting fundamental rights;

c. Protects minors online by prohibiting platforms from using targeted advertising based on the use of minors' personal data as defined in EU law;

d. Imposes certain limits on the presentation of advertising and on the use of sensitive personal data for targeted advertising, including gender, race and religion;

e. Bans misleading interfaces known as 'dark patterns', and practices aimed at misleading.

2. The Digital Markets Act will enter into force in May 2023. It affects "gatekeeper platforms" like Google, Amazon and Meta, and covers the need for user consent before processing personal data for targeted advertising.

It is interesting that most of the companies that are affected by the EU Digital Markets Act and the EU Digital Services Act are based in the United States of America.

The DMA builds a digital level playing field with clear rights and rules for large online platforms ('gatekeepers'), and ensures that gatekeepers do not abuse their position. Most provisions of the regulation apply from 2 May 2023 (Article 54, Entry into force and application). Some provisions apply from 1 November 2022.

According to Article 2 of the Digital Markets Act (DMA), 'core platform service' means any of the following:

(a) online intermediation services;

(b) online search engines;

(c) online social networking services;

(d) video-sharing platform services;

(e) number-independent interpersonal communications services;

(f) operating systems;

(g) web browsers;

(h) virtual assistants;

(i) cloud computing services;

(j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i).

According to Article 3 of the Digital Markets Act (DMA), an undertaking shall be designated as a gatekeeper if:

1. (a) it has a significant impact on the internal market;

(b) it provides a core platform service which is an important gateway for business users to reach end users; and

(c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.

An undertaking shall be presumed to satisfy the respective requirements in paragraph 1:

(a) as regards paragraph 1, point (a), where it achieves an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years, or where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States;

(b) as regards paragraph 1, point (b), where it provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least 10,000 yearly active business users established in the Union, identified and calculated in accordance with the methodology and indicators set out in the Annex;

3. The NIS 2 Directive is a major challenge for EU and non-EU companies. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall apply those measures from 18 October 2024.

According to Article 20 (Governance), the management bodies of essential and important entities must approve the cybersecurity risk-management measures taken by those entities, oversee its implementation and "can be held liable for infringements."

According to Article 20, Member States shall ensure that the "members of the management bodies of essential and important entities are required to follow training," and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

According to Article 21 (Cybersecurity risk-management measures), essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Important note for Non-EU entities: Under Article 26 (Jurisdiction and territoriality), if an entity is not established in the EU, but offers services within the EU, it shall designate a representative in the EU. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established.

In the absence of a representative, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.

4. The Critical Entity Resilience Directive (CER). By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall apply those measures from 18 October 2024. The new rules will strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

11 sectors are covered: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space and food.

EU Member States will need to adopt a national strategy and carry out regular risk assessments to identify entities that are considered critical or vital for the society and the economy.

The above are just 4 out of many compliance challenges for EU and non-EU countries. We monitor the developments in 16 risk and compliance management areas in the EU, from our sister company, Cyber Risk GmbH in Switzerland, and I feel guilty for not having the time to carefully study the regulation on markets in crypto-assets (MiCA). We need patience and time.

Leo Tolstoy believed that the two most powerful warriors are patience and time. I really wonder how our so smart friends and good people (most of them), the Russians, made such a huge mistake with this war, that is changing Europe.

In the EU, they follow what Aristophanes believed: “Men of sense often learn from their enemies. It is from their foes, not their friends, that cities learn the lesson of building high walls and ships of war.”

Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP

Number 1 (Page 8)

Financial Stability Institute, FSI Insights on policy implementation No 48

When the music stops – holding bank executives accountable for misconduct

By Rita Oliveira, Ruth Walters and Raihan Zamil

Number 2 (Page 11)

EBA publishes methodology and draft templates for the 2023 EU-wide stress test

Number 3 (Page 13)

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

Number 4 (Page 17)

European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework

European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

Number 5 (Page 23)

Agencies issue joint statement on liquidity risks resulting from crypto-asset market vulnerabilities

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

Number 6 (Page 26)

Agencies issue 2022 Shared National Credit Program review

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

Number 7 (Page 29)

Making the most of Europe's opportunities: Reforms for greater prosperity and stability

Dr Joachim Nagel, President of the Deutsche Bundesbank, at the German Institute for Economic Research (DIW), Berlin.

Number 8 (Page 31)

JP-23-01 - Sustained activity by specific threat actors

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

10 years CERT-EU

Joint Publication
Structured Cooperation between CERT-EU and ENISA
TLP:CLEAR | 15/02/2023 | JP-23-01 | v1.0

Number 9 (Page 34)

Developing National Vulnerabilities Programmes

enisa European Network and Information Security Agency

Number 10 (Page 37)

ACE Program's AI Agents Transition from Simulation to Live Flight

Artificial intelligence air combat algorithms

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Financial Stability Institute, FSI Insights on policy implementation No 48

When the music stops – holding bank executives accountable for misconduct

By Rita Oliveira, Ruth Walters and Raihan Zamil

BIS

Two lasting imprints of the Great Financial Crisis (GFC) were widespread failures in corporate governance and systemic breakdowns in corporate accountability and ethics.

The result was a toxic mix of bank failures or near failures that triggered financial instability and a global recession, causing widespread job losses and public bailouts of large financial firms.

Amid the economic downturn, a cascade of misconduct scandals emerged, eroding public confidence in banks and fuelling societal anger.

As misconduct cases proliferated, supervisory authorities encountered obstacles in determining the culpability of senior executives, particularly in large banks.

The dispersion of responsibility of senior executives in large firms, where decisions are taken at various levels of the firm, made it difficult to determine accountability where the wrongdoing may have occurred "under their watch".

In addition, many prudential authorities viewed the board of directors and senior management as collective bodies and senior executives could take cover under collective decision-making.

Following the GFC, international bodies began work to strengthen the accountability of senior executives.

In 2015, the Basel Committee on Banking Supervision (BCBS) updated its corporate governance guidelines for banks (BCBS (2015)), which included a provision for supervisors to issue guidance on the clear allocation of responsibilities, accountability and transparency of a bank's senior executives.

Subsequently, the Financial Stability Board (FSB) published a toolkit to enhance oversight of misconduct risk, including the advent of bespoke regimes that tackle individual accountability (FSB (2018)).

This paper outlines the contours of regulatory frameworks that govern the oversight of individual accountability in six jurisdictions and explores their implementation challenges. Aside from one jurisdiction, the findings draw from an FSI survey combined with follow-up interviews. This was supplemented by a review of relevant publications in all six jurisdictions.

To date, only three authorities have introduced specific, standalone frameworks that tackle individual accountability in banks. Most authorities use general prudential frameworks to address personal accountability, with one authority using a hybrid approach that combines aspects of both standalone and prudential frameworks.

For analytical purposes, we identify two broad approaches: the introduction of free-standing, consolidated "individual accountability regimes" (referred to as "IAR jurisdictions") and reliance on broader regulatory frameworks, including hybrid approaches, to hold individuals to account ("other approaches to accountability").

The three IAR jurisdictions share core features that distinguish them from other approaches to accountability, providing a solid foundation for supervisory review.

First, IARs focus on senior executives ("covered individuals").

Second, firms are required to define and allocate certain responsibilities to covered individuals, produce "accountability statements" for each of them and develop firm-wide "responsibility maps".

Third, covered individuals can be held accountable for failings in their areas of responsibility unless they have taken "reasonable steps" to prevent breach(es) from occurring.

These provisions heighten the focus on individual accountability at the highest levels of a bank, while enabling supervisors to promptly identify the senior executive(s) responsible when a supervisory concern arises and, if warranted, to hold them accountable for actions taken by their subordinates.

Despite the similarities, differences exist among the three IARs. While all three regimes cover senior roles, the treatment of non-executive directors (NEDs) varies.

These range from including NEDs (Australia), excluding NEDs (Singapore) or including a subset of NEDs (United Kingdom (UK)) within the scope of application.

The latter is the only jurisdiction that imposes heightened conduct standards on senior executives relative to other staff and prescribes certain responsibilities that must be allocated to a senior executive(s).

Finally, both Singapore and the UK extend their IARs beyond senior executives to include staff whose activities may cause material harm to the bank or consumers.

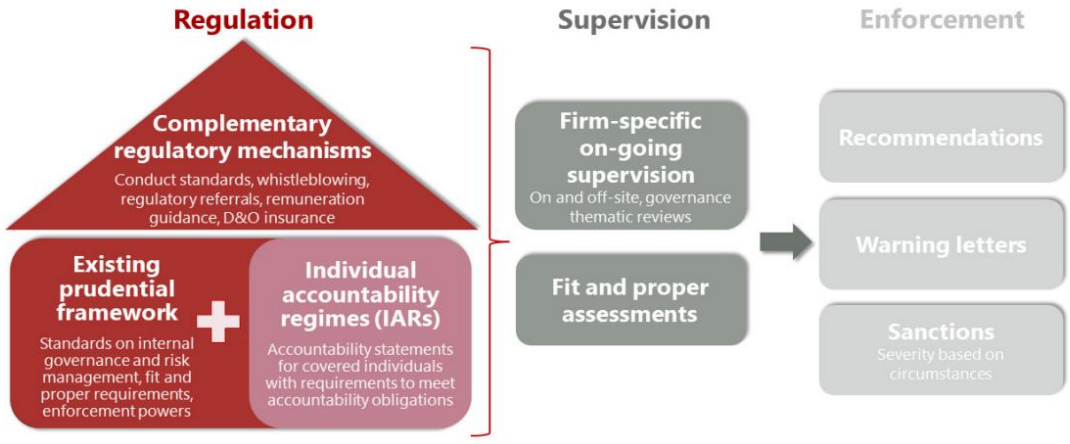
Regulatory approaches also vary among the jurisdictions without a specific IAR. The Single Supervisory Mechanism (SSM) of the European Central Bank considers individual accountability mainly during fit and proper (FAP) assessments, which applies to some senior roles.

Hong Kong SAR and the United States assess individual accountability during ongoing supervision, using common law definitions of "duty of care", "duty of loyalty" and broader prudential guidance, under which senior executives can be held accountable for misconduct.

Of the three jurisdictions without a specific IAR for banks, Hong Kong SAR comes closest, as its framework contains several elements that we identify as characterising IARs.

Of all six authorities, the US casts the broadest net, extending the reach of accountability to encompass banks' senior executives, their staff and bank-affiliated parties such as significant shareholders.

Components of individual accountability supervision — Graph 1



To read more: https://www.bis.org/fsi/publ/insights48.pdf

Number 2

EBA publishes methodology and draft templates for the 2023 EU-wide stress test

The European Banking Authority (EBA) published the final methodology, draft templates and template guidance for the 2023 EU-wide stress test along with the milestone dates for the exercise.

The methodology and templates cover all relevant risk areas and have considered the feedback received from industry. The stress test exercise will be launched in January 2023 with the publication of the macroeconomic scenarios. The results will be published by the end of July 2023.

The 2023 EU-wide stress test uses a constrained bottom-up approach with some top-down elements. Balance sheets are assumed to be constant. Focus is on the assessment of the impact of adverse shocks on banks' solvency.

Banks are required to estimate the evolution of a common set of risks (credit, market, counterparty, and operational risk) under an adverse scenario. Banks are also asked to project the impact of the scenarios on main income sources.

For net fee and commission income, risk weights of securitisation, and the credit loss path of sovereign exposures, banks are required to make use of prescribed parameters. The methodology includes the sample of banks participating in the exercise.

The stress test templates along with a template guidance are published in their draft versions as they can still be subject to minor technical adjustments before their final publication.

Milestone for the 2023 EU-wide stress test

1. Launch of the exercise at the end of January 2023;
2. First submission of results to the EBA at the beginning of April 2023;
3. Second submission to the EBA in mid-May 2023;
4. Third submission to the EBA at the end of June 2023;
5. Final submission to the EBA in mid-July 2023;

6. Publication of results by end-July 2023.

ECB-PUBLIC

ESRB
European Systemic Risk Board
European System of Financial Supervision

Macro-financial scenario for the 2023 EU-wide banking sector stress test

To read more:
https://www.eba.europa.eu/eba-publishes-methodology-and-draft-templates-2023-eu-wide-stress-test

Number 3

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

This letter was submitted to G20 Finance Ministers and Central Bank Governors (FMCBG) ahead of the G20's meeting on 24-25 February.

FSB FINANCIAL STABILITY BOARD

THE CHAIR

20 February 2023

To G20 Finance Ministers and Central Bank Governors

The financial stability outlook remains challenging. While expectations of a 'soft landing' for the global economy have grown, the outlook remains clouded by uncertainty.

The combination of near record-high levels of debt, rising debt service costs and stretched asset valuations in some key markets can pose serious threats to financial stability.

The letter lays out the FSB's work during 2023 to monitor and address these conjunctural vulnerabilities, as well as a number of structural vulnerabilities.

The letter introduces the reports the FSB is delivering to the February G20 FMCBG meeting, which cover:

The financial stability aspects of commodity markets, which forms part of the FSB's work programme to strengthen the resilience of the NBFI sector.

The financial stability risks of decentralised finance (DeFi), a fast-growing segment of the crypto-asset ecosystem. The report forms part of the FSB's work programme, jointly with sectoral standard setters, for the delivery of a consistent and comprehensive regulatory framework for crypto-assets.

Priority actions for achieving the G20 targets for enhancing cross-border payments. The report contains a detailed set of next steps to achieve the G20 cross-border payments roadmap's goals and is being accompanied by the establishment of two new taskforces to work in partnership with the private sector.

The letter also outlines forthcoming work to enhance cyber and operational resilience; and to address climate-related financial risks, through the FSB's climate roadmap.

Crypto-assets and decentralised finance

The events of the past year, such as the collapse of FTX, have highlighted the intrinsic volatility and structural vulnerabilities of crypto-assets.

We have now seen first-hand that the failure of a key intermediary in the crypto-asset ecosystem can quickly transmit risks to other parts of that ecosystem. And, if linkages to traditional finance grow, risks from crypto-asset markets could spill over onto the broader financial system.

The G20 has charged the FSB with coordinating the delivery of an effective and comprehensive regulatory framework for cryptoassets, for which we and the sectoral standard setters have jointly put forth an ambitious 2023 work programme.

This year, the FSB will finalise its recommendations for the regulation, supervision and oversight of crypto-assets and markets and its recommendations targeted at global stablecoin arrangements, which have characteristics that may make threats to financial stability more acute.

The recommendations for global stablecoin arrangements include guidance to strengthen governance frameworks, clarify and strengthen the redemption rights and the need to maintain effective stabilisation mechanisms, among other revisions.

Importantly, the FSB's work concludes that many existing stablecoins would not currently meet these high-level recommendations, nor would they meet the international standards and supplementary, more detailed BIS Committee on Payments and Market Infrastructures-International Organization of Securities Commissions guidance.

Collectively, these recommendations seek to promote the comprehensiveness and international consistency of regulatory and supervisory approaches, recognizing that many crypto-asset activities and markets are currently not compliant with applicable regulations or are

unregulated. We are working with our members, including the sectoral standard-setting bodies, to complete this critical work.

Additionally, we will deliver a joint paper with the IMF later this year that synthesises the policy findings from IMF work on macroeconomic and monetary issues and FSB work on supervisory and regulatory issues associated with cryptoassets.

We will also explore how to address the cross-border risks specific to EMDEs. Publication of the FSB's recommendations will only be the beginning of the next phase of work in this area, as the standard-setting bodies will need to make their own, more detailed, recommendations, and member jurisdictions will need to implement the recommendations.

The FSB will continue to coordinate that work, as necessary, and going forward will monitor implementation of the recommendations together with the standard-setters.

Once the work is completed, the appropriate regulation of crypto-assets, based on the principle of 'same activity, same risk, same regulation' will provide the beginning of a strong basis for harnessing potential benefits associated with this form of financial innovation while containing its risks.

Within the crypto-asset ecosystem, so-called decentralised finance (DeFi) has emerged as a fast-growing segment, and we are delivering to this meeting a report on DeFi.

Our report points to the need for proactive monitoring, filling data gaps, and exploring to what extent the cryptoasset recommendations may need to be enhanced to cover DeFi risks.

We will build on this work to examine whether additional policy recommendations are needed to deal with this growing segment.

The FSB continues to conduct forward-looking analysis to assess the implications of cryptoassets for financial stability.

This year we are undertaking in-depth analysis of the large cryptoasset intermediaries that provide a wide range of services to the ecosystem.

We will also undertake analysis of the increasing trend toward the tokenisation of assets and how that could affect financial stability.

Enhancing cross-border payments

One factor that has helped spur the development of the crypto-asset ecosystem is dissatisfaction with the existing system of cross-border payments.

In 2020, G20 Leaders endorsed the Roadmap for Enhancing Cross-border Payments, in order to address the frictions that such payments currently face and thereby achieve faster, cheaper, more transparent and more inclusive cross-border payment services.

Last year we reported to the G20 that this work had reached the next phase, focused on implementation.

For this meeting, the FSB is delivering a report with detailed next steps under the new phase of the Roadmap, comprising high-priority, practical steps to achieve the Roadmap's goals.

This is being accompanied by the setting up of two new taskforces to work in partnership with the private sector as we take the work forward. Continued G20 support remains vital here.

To read more: https://www.fsb.org/wp-content/uploads/P200223-1.pdf

Number 4

European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework

European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

DRAFT MOTION FOR A RESOLUTION, to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))
Juan Fernando López Aguilar, on behalf of the Committee on Civil Liberties, Justice and Home Affairs

The European Parliament,

– having regard to the Charter of Fundamental Rights of the European Union ('the Charter'), in particular Articles 7, 8, 16, 47 and 52 thereof,

– having regard to the judgment of the Court of Justice of 6 October 2015 in Case C-362/14 Maximillian Schrems v Data Protection Commissioner ('Schrems I'),

– having regard to the judgment of the Court of Justice of 16 July 2020 in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'),

– having regard to its enquiry into the revelations made by Edward Snowden on the electronic mass surveillance of EU citizens, including the findings in its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,

– having regard to its resolution of 26 May 2016 on transatlantic data flows,

– having regard to its resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18,

– having regard to the Commission draft Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework,

– having regard to President of the United States' Executive Order 14086 of 7 October 2022 on Enhancing Safeguards For United States Signals Intelligence Activities,

– having regard to the Regulation on the Data Protection Review Court issued by the US Attorney General ('AG Regulation'),

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR'), in particular Chapter V thereof,

– having regard to the Commission proposal of 10 January 2017 for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010), to the decision to enter into interinstitutional negotiations confirmed by Parliament's plenary on 25 October 2017, and to the Council's general approach adopted on 10 February 2021 (6087/21),

– having regard to the European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and to the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures,

– having regard to the EDPB Opinion of [to be added],

– having regard to Rule 132(2) of its Rules of Procedure,

A. whereas in the 'Schrems I' judgment, the Court of Justice of the European Union (CJEU) invalidated the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour

privacy principles and related frequently asked questions issued by the US Department of Commerce, and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to confidentiality of communications provided for in Article 7 of the Charter;

B. whereas in the 'Schrems II' judgment, the CJEU invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield and concluded that it did not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47 of the Charter;

C. whereas on 7 October 2022, the President of the United States of America signed Executive Order 14086 on Enhancing Safeguards For United States Signals Intelligence Activities ('EO');

D. whereas on 13 December 2022 the Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework;

E. whereas, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the rules applicable in that country deriving from its domestic law or its international commitments, as well as the practice designed to ensure compliance with those rules;

F. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness; whereas these transfers should be carried out in full respect for the right to the protection of personal data and the right to privacy; whereas one of the fundamental objectives of the EU is the protection of fundamental rights, as enshrined in the Charter;

G. whereas the GDPR applies to all companies processing the personal data of data subjects in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour as far as their behaviour takes place within the Union;

H. whereas mass surveillance, including the bulk collection of data, by state actors is detrimental to the trust of European citizens and businesses in digital services and, by extension, in the digital economy;

I. whereas controllers should always be accountable for compliance with data protection obligations, including demonstrating compliance for any data processing whatever its nature, scope, context, purposes and risks for data subjects;

J. whereas there is no federal privacy and data protection legislation in the United States (US); whereas the EU and the US have differing definitions of key data protection concepts such as principles of necessity and proportionality;

1. Recalls that privacy and data protection are legally enforceable fundamental rights enshrined in the Treaties, the Charter and the European Convention of Human Rights, as well as in laws and case-law; emphasises that they must be applied in a manner that does not unnecessarily hamper trade or international relations, but can be balanced only against other fundamental rights and not against commercial or political interests;

2. Acknowledges the efforts made in the EO to lay down limits on US Signals Intelligence Activities, by referring to the principles of proportionality and necessity, and providing a list of legitimate objectives for such activities; points out, however, that these principles are long-standing key elements of the EU data protection regime and that their substantive definitions in the EO are not in line with their definition under EU law and their interpretation by the CJEU; points out, furthermore, that for the purposes of the EU-US Data Privacy Framework, these principles will be interpreted solely in the light of US law and legal traditions; points out that the EO requires that signals intelligence must be conducted in a manner proportionate to the 'validated intelligence priority', which appears to be a broad interpretation of proportionality;

3. Regrets the fact that the EO does not prohibit the bulk collection of data by signals intelligence, including the content of communications; notes that the list of legitimate national security objectives can be expanded by the US President, who can determine not to make the relevant updates public;

4. Points out that the EO does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements;

5. Points out that the decisions of the Data Protection Review Court ('DPRC') will be classified and not made public or available to the complainant; points out that the DPRC is part of the executive branch and not the judiciary; points out that a complainant will be represented by a 'special advocate' designated by the DPRC, for whom there is no

requirement of independence; points out that the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data; notes that the proposed redress process does not provide for an avenue for appeal in a federal court and therefore, among other things, does not provide any possibility for the complainant to claim damages; concludes that the DPRC does not meet the standards of independence and impartiality of Article 47 of the Charter;

6. Notes that, while the US has provided for a new mechanism for remedy for issues related to public authorities' access to data, the remedies available for commercial matters under the adequacy decision are insufficient; notes that these issues are largely left to the discretion of companies, which can select alternative remedy avenues such as dispute resolution mechanisms or the use of companies' privacy programmes;

7. Notes that European businesses need and deserve legal certainty; stresses that successive data transfer mechanisms, which were subsequently repealed by the CJEU, created additional costs for European businesses; notes that continuing uncertainty and the need to adapt to new legal solutions is particularly burdensome for micro, small and medium-sized enterprises;

8. Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the US still does not have a federal data protection law; points out that the EO is not clear, precise or foreseeable in its application, as it can be amended at any time by the US President; is therefore concerned about the absence of a sunset clause which could provide that the decision would automatically expire four years after its entry into force;

9. Emphasises that adequacy decisions must include clear and strict mechanisms for monitoring and review in order to ensure that decisions are future proof and that EU citizens' fundamental right to data protection is guaranteed;

Conclusions

10. Recalls that, in its resolution of 20 May 2021, Parliament called on the Commission not to adopt any new adequacy decision in relation to the US, unless meaningful reforms were introduced, in particular for national security and intelligence purposes;

11. Concludes that the EU-US Data Privacy Framework fails to create actual equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU; urges the Commission not to adopt the adequacy finding;

12. Instructs its President to forward this resolution to the Council, the Commission and the President and Congress of the United States of America.

Number 5

Agencies issue joint statement on liquidity risks resulting from crypto-asset market vulnerabilities

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing this statement on the liquidity risks presented by certain sources of funding from crypto-asset-related entities, and some effective practices to manage such risks.

The statement reminds banking organizations to apply existing risk management principles; it does not create new risk management principles.

Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

Liquidity Risks Related to Certain Sources of Funding from Crypto-Asset-Related Entities

This statement highlights key liquidity risks associated with crypto-assets and cryptoasset sector participants that banking organizations should be aware of.

In particular, certain sources of funding from crypto-asset-related entities may pose heightened liquidity risks to banking organizations due to the unpredictability of the scale and timing of deposit inflows and outflows, including, for example:

1. *Deposits placed by a crypto-asset-related entity that are for the benefit of the crypto-asset-related entity's customers (end customers).* The stability of such deposits may be driven by the behavior of the end customer or crypto-asset sector dynamics, and not solely by the crypto-asset-related entity itself, which is the banking organization's direct counterparty.

The stability of the deposits may be influenced by, for example, periods of stress, market volatility, and related vulnerabilities in the crypto-asset sector, which may or may not be specific to the crypto-asset-related entity.

Such deposits can be susceptible to large and rapid inflows as well as outflows, when end customers react to crypto-asset-sector-related market events, media reports, and uncertainty.

This uncertainty and resulting deposit volatility can be exacerbated by end customer confusion related to inaccurate or misleading representations of deposit insurance by a crypto-asset related entity.

2. *Deposits that constitute stablecoin-related reserves*. The stability of such deposits may be linked to demand for stablecoins, the confidence of stablecoin holders in the stablecoin arrangement, and the stablecoin issuer's reserve management practices.

Such deposits can be susceptible to large and rapid outflows stemming from, for example, unanticipated stablecoin redemptions or dislocations in crypto-asset markets.

More broadly, when a banking organization's deposit funding base is concentrated in crypto-asset-related entities that are highly interconnected or share similar risk profiles, deposit fluctuations may also be correlated, and liquidity risk therefore may be further heightened.

Effective Risk Management Practices

In light of these heightened risks, it is important for banking organizations that use certain sources of funding from crypto-asset-related entities, such as those described above, to actively monitor the liquidity risks inherent in such funding sources and establish and maintain effective risk management and controls commensurate with the level of liquidity risks from such funding sources.

Effective practices for these banking organizations could include, for example:

• Understanding the direct and indirect drivers of potential behavior of deposits from crypto-asset-related entities and the extent to which those deposits are susceptible to unpredictable volatility.

• Assessing potential concentration or interconnectedness across deposits from cryptoasset-related entities and the associated liquidity risks.

• Incorporating the liquidity risks or funding volatility associated with crypto-asset related deposits into contingency funding planning, including liquidity stress testing and, as appropriate, other asset-liability governance and risk management processes.

• Performing robust due diligence and ongoing monitoring of crypto-asset-related entities that establish deposit accounts, including assessing the representations made by those crypto-asset-related entities to their end customers about such deposit accounts that, if inaccurate, could lead to rapid outflows of such deposits.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20230223a.htm

Number 6

Agencies issue 2022 Shared National Credit Program review

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

The federal bank regulatory agencies reported in the 2022 Shared National Credit (SNC) report that credit quality associated with large syndicated bank loans improved in 2022, but noted the results do not fully reflect increasing interest rates and softening economic conditions that began to impact borrowers in the second half of 2022.

Overall, the report finds that credit risks for syndicated loans—large loans originated by multiple banks—were moderate at the end of the review period. While risks to borrowers impacted by COVID-19 have declined, they remain high for leveraged loans, as well as the entertainment, recreation, and transportation services industries.

The 2022 review, which evaluates the quality of large, syndicated loans, was conducted by the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, and reflects the examination of SNC loans originated on or before June 30, 2022.

Consistent with the approach taken in 2021, it focused on borrowers in five industries that were affected significantly by the pandemic: entertainment and recreation; oil and gas; commercial real estate; retail; and transportation services.

The 2022 SNC portfolio included 6,214 borrowers, totaling $5.9 trillion in commitments, an increase of 13.9 percent from a year ago. The percentage of loans that deserve management's close attention (loans rated non-pass, including special mention and classified SNC commitments) decreased from 10.6 percent of total commitments to 7.0 percent year over year.

Nearly half of total SNC commitments are leveraged loans, and commitments to borrowers in industries affected by COVID-19 represent about one-fifth of total SNC commitments.

For leveraged borrowers that also operate in COVID-19 affected industries, non-pass loans decreased to 18.9 percent, but remain above the 13.5 percent observed in 2019.

While U.S. banks hold nearly 45 percent of all SNC commitments, they hold only 21 percent of non-pass loans.

About the Shared National Credit Program

The Shared National Credit (SNC) Program assesses risk in the largest and most complex credit facilities shared by multiple regulated financial institutions.

The SNC Program is governed by an interagency agreement among the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (the agencies).

The program began in 1977 to review borrowers with minimum aggregate loan commitments totaling $20 million or more that were shared by two or more regulated financial institutions (banks).

A program modification in 1998 increased the minimum number of regulated financial institutions from two to three.

To adjust for inflation and changes in average loan size, the agencies increased the minimum aggregate loan commitment threshold from $20 million to $100 million effective January 1, 2018.

SNC reviews are completed in the first and third quarters of the calendar year. Large agent banks receive two reviews each year while a selection of other agent banks receive a single review each year.

The results discussed in this document reflect reviews conducted in the first and third quarters of 2022, and primarily cover loan commitments originated on or before June 30, 2022.

Trends and exhibits shown in the report include outstanding loans and commitments by all reporting banks.

Although some banks are reviewed twice a year, the agencies will continue to issue a single statement annually that captures combined findings from the previous 12 months.

The next statement will be released upon completion of the third quarter 2023 SNC review.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230224a1.pdf

Number 7

Making the most of Europe's opportunities: Reforms for greater prosperity and stability

Dr Joachim Nagel, President of the Deutsche Bundesbank, at the German Institute for Economic Research (DIW), Berlin.

Introduction

Ladies and gentlemen, I am delighted to be with you all here today at the German Institute for Economic Research (DIW) in Berlin to give this DIW Europe Lecture.

Nowadays, it is almost impossible to talk about Europe without thinking about Ukraine. This attack not only marked a much discussed turning point, but it also has shown us, in brutally obvious terms, the devastation caused by war. People have been fleeing from missiles, losing all of their possessions, and mourning their loved ones.

With this in mind, everything that has been achieved since the end of the Second World War seems no less than a miracle. After Germany's atrocities, Europe was in ruins. Today, formerly hostile countries such as Germany and France are joined in union. Together, we have achieved peace, freedom and prosperity. And, in the European Union, we have also created a community of values.

This union is based on a political vision. It was created and advanced by figures such as Jean Monnet, Konrad Adenauer and Jacques Delors. I will be discussing all three of them later in my speech.

However, this unification process has been essentially achieved not least through the convergence of national economies. And this has been true since the very outset. For example, consider the Schuman Declaration of 1950. It led to the founding of the European Coal and Steel Community. Seven years thereafter, the Treaties of Rome expanded the single market beyond the coal, iron and steel industry.

On this subject, Konrad Adenauer said: "The common market must not be regarded first and foremost as an economic treaty, but as a political instrument [...] that aims to reach a politically integrated Europe by means of mutual economy."

The common market was to be based on the free movement of goods, persons, services, and capital. However, it would take a while longer until these four freedoms became more of a reality: in 1986, the Single European Act created the conditions for extensive reform processes. This was followed by a comprehensive programme of reforms. Economic integration then entered a new phase in 1993, when the European single market, as we know it today, came into existence.

30 years later, I think we can say that it was all worth it. The single market is truly a source of prosperity. However, it is still far from achieving its fullest potential. We can benefit from the single market more than ever before. But how? This is what I would like to talk about today.

It will be about giving the single market new impetus. In my view, there are three main areas of action in this regard: services, digitalisation, and the capital market. As a central banker, I have a particular interest in the capital markets union and the opportunities offered by a digital euro.

Then, to conclude, I will speak on the subject of EU fiscal rules. Though they are not part of the single market, they are a cornerstone of stable monetary union – and, as you may know, their reform is currently on the agenda.

To read more:
https://www.bundesbank.de/en/press/speeches/making-the-most-of-europe-s-opportunities-reforms-for-greater-prosperity-and-stability-904952

Number 8

JP-23-01 - Sustained activity by specific threat actors

Joint Publication
Structured Cooperation between CERT-EU and ENISA
TLP:CLEAR | 15/02/2023 | JP-23-01 | v1.0

Summary

The EU Cybersecurity Agency (ENISA) and the CERT for the EU institutions, bodies and agencies (CERT-EU) would like to draw the attention of their respective audiences on particular Advanced Persistent Threats (APTs), known as APT27, APT30, APT31, Ke3chang, GALLIUM and Mustang Panda.

These threat actors have been recently conducting malicious cyber activities against business and governments in the Union.

On 19 July 2021, the EU has urged Chinese authorities to take actions against malicious cyber activities undertaken from their territory, and linked to APT31. These malicious cyber activities, which had significant effects, targeted government institutions and political organisations in the EU and Member States, as well as key European industries.

On 18 July 2022, Belgium has also urged Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors. These activities can be linked to the hacker groups known as APT 27, APT 30, APT 31, and GALLIUM.

Moreover, commercial firms indicated that Ke3chang and Mustang Panda are likely operating from the territory of China.

These threat actors present important and ongoing threats to the European Union. Recent operations pursued by these actors focused mainly on information theft, primarily via establishing persistent footholds within the network infrastructure of organisations of strategic relevance.

ENISA and CERT-EU call for all public and private sector organisations in the EU to apply the recommendations included in this document in a consistent and systematic manner.

These recommendations aim to reduce the risk of being compromised by the mentioned APTs, as well as substantially improve the cybersecurity posture and enhance the overall resilience of these organisations against cyberattacks.

Recommendations

All public and private sector organisations in the EU are strongly advised to follow common cyber hygiene recommendations.

Our previously published best practices and the corresponding security guidance provide a solid basis for mitigating cyberattacks.

CERT-EU Security Guidance 22-001

Cybersecurity mitigation measures against critical threats

You may visit:
https://www.cert.europa.eu/static/WhitePapers/TLP-WHITE-CERT-EU_Security_Guidance-22-001_v1_0.pdf

Following the analysis of the available information on the aforementioned threat actors (see below) and of some of their major tactics, techniques, and procedures, ENISA and CERT-EU draw a number of complementary recommendations to foster the defensive capabilities of the intended audience.

Each organisation which wants to apply these recommendations is fully responsible for the implementation, according to its business needs and priorities.

Additionally, CERT-EU and ENISA emphasise the importance of participating in information sharing communities and reviewing your national/governmental CSIRT's security guidance and public resources detailing tactics, techniques and procedures associated with the threat actors.

Name	Likely motive	Examples of associated tools
APT27 (aka Lucky Mouse, Emissary Panda, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, Bronze Union)	Information theft; ransomware operation	Ghost, ASPXSpy, ZxShell RAT, HyperBro, PlugX RAT, Windows Credential Editor, FoundCore, China Chopper, gsecdump, HTTPBrowser, Impacket, ipconfig, Mimikatz, NBTscan, Net, OwaAuth, pwdump, ZxShell.
Threat actor description		
APT27 has been observed targeting a broad range of organisations across a wide geographic area, including Europe, North and South America, Africa, the Middle East, and the Asia Pacific (APAC) region. The group has been primarily observed conducting watering hole and spear-phishing attacks as its key means of gaining initial footholds within target networks [7]. Since 2020, APT27 operators have also been observed engaging in ransomware-based cybercriminal activities, suggesting members of the group may be conducting financially motivated activity, in addition to standard exfiltration-driven activities [8]. APT27 is also known for its high degree of operational sophistication and frequently alters its attack strategies. In order to obfuscate its their activities, evade detection and maintain long-term network persistence, APT27 deploys fileless malware and pivots within the target networks. Incidents linked to APT27 have also been recorded alongside clusters of activity from other threat groups, assessed to be operating from the same nation state such as APT30, APT31, and GALLIUM.		

Aktuelle Cyberangriffskampagne gegen deutsche Wirtschaftsunternehmen durch die Gruppierung APT27

Aktuelle Erkenntnisse deuten auf anhaltende Cyberangriffsaktivitäten der Gruppierung APT27 gegen Wirtschaftsunternehmen in Deutschland hin.

Sachverhalt

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse über eine anhaltende Cyberspionagekampagne durch die Cyberangriffsgruppierung APT27 unter Einsatz der Schadsoftwarevariante HYPERBRO gegen deutsche Wirtschaftsunternehmen vor. Nach aktuellen Erkenntnissen nutzen die Angreifer seit März 2021 Schwachstellen in Microsoft Exchange sowie in der Software Zoho AdSelf Service Plus[1] als Einfallstor für die Angriffe aus.

Es kann nicht ausgeschlossen werden, dass die Akteure neben dem Diebstahl von Geschäftsgeheimnissen und geistigem Eigentum versuchen, die Netzwerke der (Unternehmens-)Kunden beziehungsweise von Dienstleistern zusätzlich zu infiltrieren (Supply-Chain-Angriff).

To read more:
https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication

Number 9

Developing National Vulnerabilities Programmes

Based on the experiences and perspectives gathered from industry players and national governments, as well as on the documentation developed by multiple actors involved with national vulnerability initiatives and programmes, the EU Coordinated Vulnerability Disclosure (CVD) ecosystem remains fragmented.

Although interesting approaches and initiatives are taking place in some EU Member States, yet further steps can be done towards an integrated EU vision and action.

This report shows that, despite recent efforts by national governments in developing CVD policies, some industry players have taken the lead and developed vulnerability policies and programmes at organisation level.

Nevertheless, among the top industry expectations is that the development of a national or European level CVD policy could help organisations and public administrations to set vulnerability management as a priority and further encourage security practices.

In addition, the alignment of such policies with existing international standards, can greatly help in promoting harmonization.

As far as vulnerability initiatives are concerned, Bug Bounties Programmes (BBP) is an area that grew remarkably over the past few years.

BBPs have considerably adapted their business models in offering different type of services, hence different coverages of IT systems and levels of involvement in vulnerability management processes.

Today, BBPs platform providers are now cooperating with key public institutions to run customised programmes adapted to their needs and IT infrastructures.

Further expansion is expected as long as the community can continue relying on BBPs (i.e., confidentiality of internal information and data protection) and ensuring trust between the stakeholders involved. In terms of human capital, researchers play a fundamental role in the disclosure of vulnerabilities.

Accordingly, it is interesting to understand motivations, incentives and challenges influencing researchers' contribution.

From their perspective, reputation remains as a one of the key incentives to legally report vulnerabilities, as it leads to fame and recognition.

However, legal protection is also highly considered, especially because the absence, uncertainty or non-clarity of legal conditions can push to illegal channels.

Collaborative challenges arise in the use of tools to improve vulnerability disclosure processes.

For example, when looking into vulnerabilities related to open-source software (OSS) and considering how intertwined commercial and OSS are today, a need to further improve coordination between OSS developers and private vendors was identified.

Aspects such as OSS vulnerability handling, responsibility and accountability are not yet clearly defined and among actors involved across the IT product supply chains, which may hinder coordination efforts.

Challenges related to technical and technological issues also constitute a key area of discussion and analysis.

A forward-looking perspective on the use of automation as an enabler to efficiently manage vulnerability identification, sourcing and classification is also provided by this report.

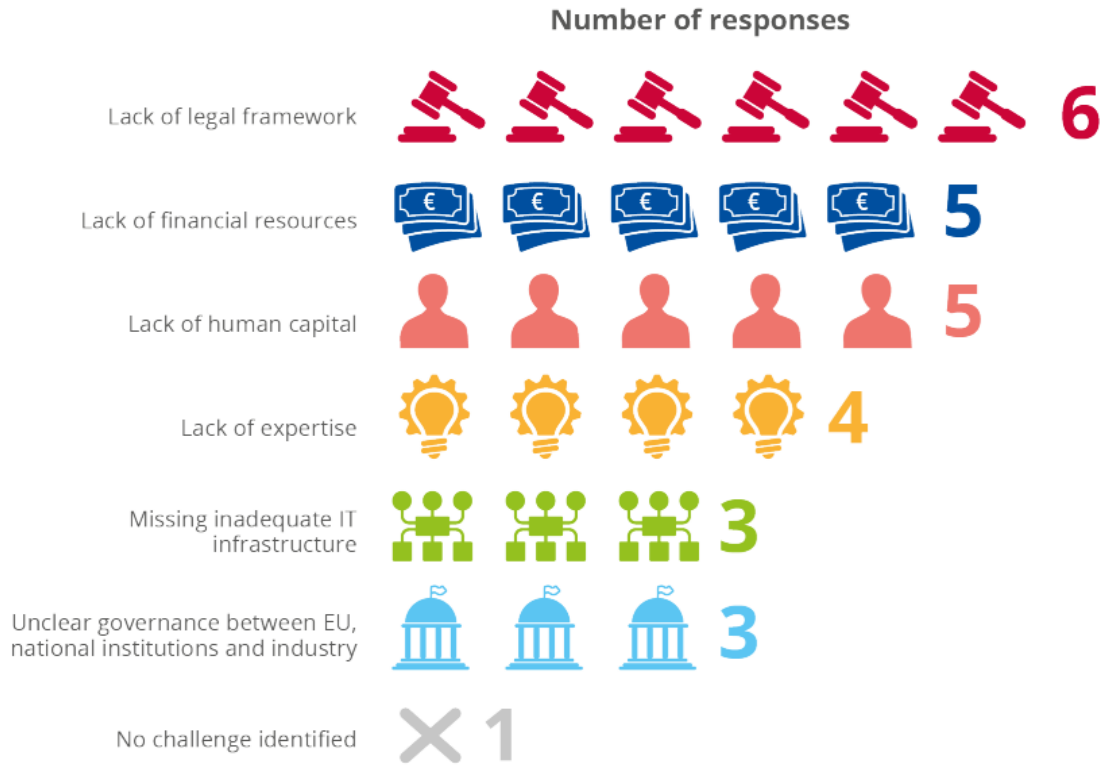
It is observed that, as vulnerability analysis and treatment still require human expertise, the risk of deskilling experts due to automated processes may be minimised.

Finally, alignment across different legislation as well as cooperation between industry players and governments are needed to avoid silos.

Harmonisation of CVD practices, coordination and international cooperation among players are essential priorities both from a legal and technical perspectives.

In this regard, ENISA will continue offering advice, publishing guidelines, promoting information sharing, raising awareness, and coordinating CVD-related activities at national and EU level.

Figure 3: Challenges encountered by stakeholders involved in coordinated vulnerability disclosure policy development and implementation



Source: Findings from interviews, Q3) What are the main challenges regarding the vulnerability policies' development and implementation? Interviewees (N=9).

To read more:
https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes

Number 10

ACE Program's AI Agents Transition from Simulation to Live Flight

Artificial intelligence air combat algorithms

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In less than three years, artificial intelligence (AI) algorithms developed under DARPA's Air Combat Evolution (ACE) program have progressed from controlling simulated F-16s flying aerial dogfights on computer screens to controlling an actual F-16 in flight.

In early December 2022, ACE algorithm developers uploaded their AI software into a specially modified F-16 test aircraft known as the X-62A or VISTA (Variable In-flight Simulator Test Aircraft), at the Air Force Test Pilot School (TPS) at Edwards Air Force Base, California, and flew multiple flights over several days. The flights demonstrated that AI agents can control a full-scale fighter jet and provided invaluable live-flight data.

The ACE AI flights were a part of a successful broader test event including DARPA, TPS, and the Air Force Research Laboratory, enabling multiple Defense Department organizations to work closely together with AI-development contractors toward shared objectives.

"Thanks to the outstanding teamwork and coordination between DARPA, the Air Force Test Pilot School, the Air Force Research Laboratory, and our performer teams, we've made rapid progress in Phase 2 across all areas of the ACE program," said Air Force Lt. Col.

Ryan "Hal" Hefron, the DARPA program manager for ACE. "VISTA allowed us to streamline the program by skipping the planned subscale phase and proceeding directly to a full-scale implementation, saving a year or more and providing performance feedback under real flight conditions."

DARPA performers EpiSci, PhysicsAI, Shield AI, and the Johns Hopkins Applied Physics Laboratory flew different F-16 AI algorithms on the X-62A. The aircraft, a highly modified two-seat F-16, can be programmed to demonstrate the flight-handling characteristics of a variety of different aircraft types.

VISTA was upgraded recently with the System for Autonomous Control of Simulation (SACS), making the aircraft a perfect platform to test ACE's autonomous F-16 AI agents. A safety pilot was on board the VISTA aircraft to take control if anything went awry.

"We conducted multiple sorties [takeoffs and landings] with numerous test points performed on each sortie to test the algorithms under varying starting conditions, against various simulated adversaries, and with simulated weapons capabilities," Hefron said.

"We didn't run into any major issues but did encounter some differences compared to simulation-based results, which is to be expected when transitioning from virtual to live. This highlights the importance of not only flight testing advanced autonomous capabilities but doing so on testbeds like VISTA, which allowed us to rapidly learn lessons and iterate at a much faster rate than with other air vehicles."

The Test Pilot School is also supporting the ACE program in measuring how well pilots trust the AI agent to conduct within-visual-range air combat (called a dogfight) while the human pilot focuses on larger battle management tasks in the cockpit.

Air Force test pilots have flown numerous live flights in L-29 jet trainers at the University of Iowa Technology Institute's Operator Performance Laboratory (OPL), an ACE performer.

The two-seat L-29 jets at OPL are outfitted with sensors in the cockpit to measure pilot physiological responses, giving researchers clues as to whether the pilot is trusting the AI or not.

The TPS recently hosted an ACE Trust Capstone event in late January 2023 using simulators to gauge pilot-agent alignment with follow-on trust-calibration flights in the X-62A planned for later this year.

Begun in 2019, ACE aims to develop trusted, scalable, human-level, AI-driven autonomy for air combat by using human-machine collaborative dogfighting as its challenge problem.

In August 2020, the ACE program's AlphaDogfight Trials pitted AI agents against each other flying simulated F-16s in a virtual dogfighting competition that culminated with the winning AI defeating an experienced F-16 fighter pilot flying in a simulator.

To read more: https://www.darpa.mil/news-events/2023-02-13

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,

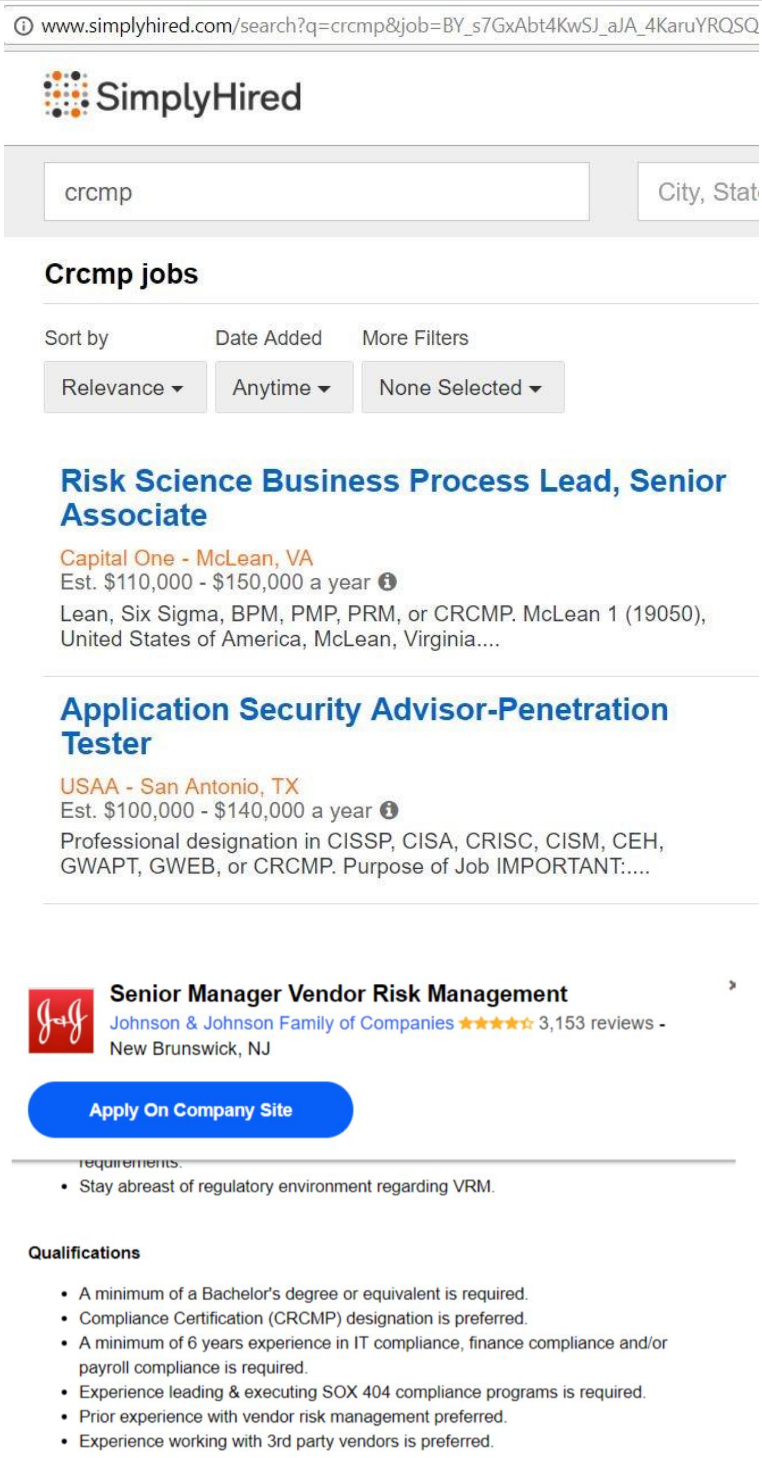
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.