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 27, 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 the EU proposal for a Regulation on Markets in Crypto-assets (also called "MiCA"). The European Commission believes that 'crypto-assets' and 'distributed ledger technology' should be defined *as widely as possible,* to capture all types of crypto-assets which currently fall *outside* the scope of EU legislation on financial services.

MiCA follows the recommendations of the Financial Action Task Force (FATF), and contributes to the objective of combating money laundering and the financing of terrorism.

Issuers of asset-referenced tokens should have robust *governance arrangements,* including a clear organisational structure with well-defined, transparent and consistent lines of responsibility and effective processes to identify, manage, monitor and report the risks to which they are or might be exposed.

The management body of such issuers and their shareholders should have good repute and sufficient expertise and be fit and proper for the purpose of anti-money laundering and combatting the financing of terrorism.

Issuers of asset-referenced tokens should also employ resources proportionate to the scale of their activities and should always ensure continuity and regularity in the performance of their activities.

For that purpose, issuers of asset-referenced tokens should establish a business continuity policy aimed at ensuring, in the case of an interruption to their systems and procedures, the performance of their core payment activities.

Issuers of asset-referenced tokens should also have a strong internal control and risk assessment mechanism, as well as a system that guarantees the integrity and confidentiality of information received. (I would not be surprised if they asked for Sarbanes-Oxley compliance too).

All jokes aside, this is an important development. The EU wants to avoid corporate governance failures like the one Sam Bankman-Fried had established in FTX. I know, crypto-assets were not exactly thought to work like that, but this is the obvious end of the road. MiCA is absolutely in line with FSB's framework for the regulation of crypto-asset activities. FSB asks for the principle of *"same activity, same risk, same regulation"*.

Where crypto-assets and intermediaries perform an equivalent economic function to one performed by instruments and intermediaries of the traditional "centralized" financial sector, they should be subject to equivalent regulation, even when they try (without much success) to become "decentralized".

Read more at number 5 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP

Number 1 (Page 5)

U.S. Department of Justice, Criminal Division

Evaluation of Corporate Compliance Programs (Updated March 2023)

Number 2 (Page 8)

New types of digital money

Signe Krogstrup, Governor of the National Bank of Denmark, at the National Bank of Denmark's conference "New types of digital money", Copenhagen.

Number 3 (Page 11)

Investor Advisory: Exercise Caution With Third-Party Verification/Proof of Reserve Reports

Number 4 (Page 14)

Joint ESAs-ECB Statement on disclosure on climate change for structured finance products

Number 5 (Page 17)

Proposal for a regulation on Markets in Crypto-assets (MiCA)

Number 6 (Page 22)

Remarks at the IIB Annual Washington Conference "Trust and Global Banking: Lessons for Crypto".

Acting Comptroller of the Currency Michael J. Hsu.

Office of the Comptroller of the Currency

Number 7 (Page 24)

Statement on Silicon Valley Bank

Bank of England

Number 8 (Page 26)

NPSA is the UK Government's National Technical Authority for Physical and Personnel Protective Security.

Security Campaigns

National Protective Security Authority

Number 9 (Page 29)

DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit

Microsoft Threat Intelligence

Microsoft

Number 10 (Page 33)

Office of the Director of National Intelligence

2023 Annual Threat Assessment of the U.S. Intelligence Community

Number 1

U.S. Department of Justice, Criminal Division

Evaluation of Corporate Compliance Programs (Updated March 2023)

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements.

These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one.").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine.

Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate

(1) form of any resolution or prosecution;

(2) monetary penalty, if any; and

(3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs.

We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation.

Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program.

There are, however, common questions that we may ask in the course of making an individualized determination.

As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?

2. Is the program being applied earnestly and in good faith?
In other words, is the program adequately resourced and empowered to function effectively?

To read more:
https://www.justice.gov/criminal-fraud/page/file/937501/download

Number 2

New types of digital money

Signe Krogstrup, Governor of the National Bank of Denmark, at the National Bank of Denmark's conference "New types of digital money", Copenhagen.

Introduction

Ladies and gentlemen. It's a pleasure to welcome you to the conference on New types of digital money here at Danmarks Nationalbank.

Digitalization, new technologies and financial innovation are changing the nature of society. They also touch at the core of central bank mandates of monetary and financial stability as well as secure and efficient payment systems.

Central banks are therefore increasingly analysing the implications for the future of the monetary and financial system. Danmarks Nationalbank is no exception. We pay close attention to ensure that society reaps the gains while minimising potential costs of these developments.

This is no simple task. Innovation in digital money and payments is moving fast and the direction is uncertain. We have to assess how to best respond to developments as they unfold. But we also need to stand ready to change our assessment when circumstances change or new insights emerge.

This is why we have convened you all to this conference today. I'm looking forward to the presentations and discussions on the agenda. As a central bank, we want to engage, we want to learn, and we want to be challenged!

But I would like to start by emphasising what we do know, from monetary history and scholarship. I will then discuss some of the implications for our assessment of future types of money.

1. Lessons from history on the functioning of money

History has plenty of examples of money that worked well and money that didn't.

For money to work well, it needs to

… be an efficient and broadly accepted means of payment.

… be the unit of account in which prices of goods and services are denominated to anchor our sense of the relative value of different goods and services.

… and finally, hold a stable predictable value, or purchasing power, over time. This is essentially what we mean by price stability.

Underlying these attributes of money is trust. You accept money as payment only when trusting that others will do so as well, now and in future.

You hold money trusting that it will maintain its purchasing power over time. Without trust, money does not function.

So, where does trust come from? In earlier monetary history, trust in the value of money was ensured in so-called "commodity money"; money with intrinsic value and use in its own right. Examples are plentiful: Cigarettes during wars, pearls or gold coins. Historically, gold had value in terms of its use for making jewellery.

The history of the gold standard illustrates a universal lesson about the value of money: the supply of money has to adjust to the demand for money for transactions, to ensure stable value and prices.

Gold did not succeed in ensuring stable prices because its supply is largely determined by production from gold mines, and not by the needs of the economy. An expanding economy without an expanding supply of money leads to deflation.

The gold standard was succeeded by fiat money. That is, money with no intrinsic value, issued by banks or monetary institutions. Unlike gold coins, the supply of fiat money is under the control of the issuer.

Herein lies both a strength and a weakness of fiat money. It can be issued to ensure stable value, but it can also be issued to cover short term financing needs of the issuer, leading to an eventual loss of value.

An often-quoted example is the 19th century US Free Banking Era. During that era, commercial banks issued their own fiat money, without a central bank issued currency. Banks were often tempted to over-issue money without sufficient backing, leading to frequent episodes of a loss of trust

and bank runs.

The temptation to over-issue has also been present during historical episodes with central banks or with governments as issuers of money. This has been the case when financing needs have dominated concerns about monetary and financial stability.

This brings me to another important lesson, namely that to maintain trust in fiat money, there has to be trust in the issuer's commitment to keep the value of money stable as the economy evolves.

The current monetary system has a strong track record of achieving this trust. In the current system, central banks as well as commercial banks issue fiat money with the same unit of account, as illustrated in the slide.

To read more:
https://www.nationalbanken.dk/en/pressroom/speeches/Pages/2023/Governor-Signe-Krogstrups-speech-at-Danmarks-Nationalbanks-conference-New-types-of-digital-money.aspx

Number 3

Investor Advisory: Exercise Caution With Third-Party Verification/Proof of Reserve Reports

Proof of reserve reports are inherently limited, and customers should exercise extreme caution when relying on them to conclude that there are sufficient assets to meet customer liabilities.

This document represents the views of the Public Company Accounting Oversight Board's (PCAOB or "Board") Office of the Investor Advocate staff and not necessarily those of the Board or other PCAOB staff. It is not a rule, policy, or statement of the Board.

The Office of the Investor Advocate is aware of some service providers, including PCAOB-registered audit firms, issuing proof of reserve reports ("PoR Reports") to certain crypto entities (e.g., crypto exchanges, stablecoin issuers).

Crypto entities may engage a service provider to issue a PoR Report in an attempt to reassure customers in response to widespread concerns about, for example, the type of reserve holdings, or, the safety and availability of customers' digital assets in the event that some or all of the customers decide to withdraw their assets (e.g., if there is a run on a crypto exchange or stablecoin issuer).

The Office of the Investor Advocate is issuing this Investor Advisory because of concerns that investors and others may place undue reliance on PoR Reports, which are not within the PCAOB's oversight authority.

Importantly, investors should note that PoR engagements are not audits and, consequently, the related reports do not provide any meaningful assurance to investors or the public.

As a general matter, these PoR Reports purport to provide an asset verification for an asset type at a particular moment in time, subject to significant limitations based on the procedures performed.

For example, the procedures undertaken likely do not address the crypto entity's liabilities, the rights and obligations of the digital asset holders, or whether the assets have been borrowed by the crypto entity to make it appear they have sufficient collateral or "reserves" in excess of customer demands.

For this reason, if the assets were borrowed by the crypto entity at the time of the PoR engagement, investors would not know based on the PoR Report.

Also, because PoR Reports concern digital assets at one point in time they do not provide any assurance about whether the assets were used, lent, or otherwise became unavailable to customers following issuance of the PoR Report.

Moreover, PoR Reports also provide no assurance regarding the effectiveness of internal controls or of governance of the crypto entity.

Despite any representations to the contrary, PoR Reports are not equivalent or more rigorous than an audit, and they are not conducted in accordance with PCAOB auditing standards.

In addition, there is a lack of uniformity regarding service providers that perform PoR engagements.

For example, some PoR engagements are performed by accounting firms, whereas others are performed by non-accountant assurance providers.

Management of the crypto entities also have discretion on whether the results of PoR reports are made public, including the extent and format of the information provided.

PoR engagements, whether intended to provide reasonable assurance, limited assurance, or no assurance (agreed-upon procedures), are not subject to PCAOB auditing standards and the engagements are not subject to PCAOB inspection.

Importantly, such reports do not provide assurance that such reserves will be adequate as of the date of the PoR Report, in the future, or that customer assets will be protected.

For “agreed-upon procedures,” the management of the crypto entity, not the provider of the PoR Report, determines the procedures to be performed by the third party when conducting the engagement.

Under these circumstances, the PoR Report provides only factual findings of the outcome of the procedures performed, and there is no representation as to the sufficiency of such procedures. These types of PoR reports do not express an opinion on the adequacy of the “reserves” or the financial stability of the crypto entity or the validity of management’s assertion(s).

Similarly, PoR engagements that purport to provide limited or reasonable assurance are not subject to uniform standards. Therefore, the manner in which the engagements are performed yield different results based on the different standards selected by management and PoR service providers.

Proof of reserve reports are inherently limited, and customers should exercise extreme caution when relying on them to conclude that there are sufficient assets to meet customer liabilities.

To read more:
https://pcaobus.org/resources/information-for-investors/investor-advisories/investor-advisory-exercise-caution-with-third-party-verification-proof-of-reserve-reports

Number 4

Joint ESAs-ECB Statement on disclosure on climate change for structured finance products

The European Supervisory Authorities1 (ESAs) and the ECB are committed to contributing to the transition towards a more sustainable economy within their respective mandates.

As investment in financial products meeting high environmental, social and governance (ESG) standards is increasingly important in the European Union (EU), it has also become a priority for structured finance products to disclose climate-related information on the underlying assets.

ESMA, with the contribution of EBA, EIOPA and the ECB, is hence working towards enhancing disclosure standards for securitised assets by including new, proportionate and targeted climate change-related information.

The ESAs and the ECB also call on issuers, sponsors and originators of such assets at EU level to proactively collect high-quality and comprehensive information on climate-related risks during the origination process.

This call for improved disclosure concerns all funding instruments that are backed by the same type of underlying assets.

Enhanced climate related data are needed for securitised assets

Securitisation transactions are often backed by assets that could be directly exposed to physical or transition climate-related risks, such as real estate mortgages or auto loans.

Since the value of these underlying assets could be affected by climate-related events, the ESAs and the ECB share the view that the reporting on existing climate-related metrics needs to improve, and that additional metrics are necessary.

Additional climate related data will allow investors to better identify climate change-related risks while avoiding overreliance on estimates from external sources. The lack of climate-related data on the assets underlying structured finance products not only poses a problem for properly assessing and addressing climate-related risks but also impedes the classification of

products and services as sustainable under the EU Taxonomy Regulation and Sustainable Finance Disclosure Regulation (SFDR).

The ESAs and the ECB are committed to supporting better and targeted disclosures for structured finance products

The ESAs are committed to promoting transparency and robust disclosure requirements for financial institutions and financial products.

The ESAs have been developing advice and Regulatory Technical Standards under the EU Taxonomy Regulation and the Sustainable Finance Disclosure Regulation.

They are also currently reviewing the SFDR Delegated Regulation to enhance ESG disclosures by financial market participants, including to require additional disclosures on decarbonisation targets.

Sustainable finance is a key priority of the ESAs, and further deepening the integration of ESG factors across their activities will be a focus for their action in the coming months and years.

Enhanced climate-related disclosure requirements for securitised assets are also essential to the ECB.

Assets-backed securities constitute one of the most important asset classes mobilised by counterparties as collateral in Eurosystem credit operations. Moreover, the Eurosystem, with its asset backed securities purchase programme (ABSPP), has also become one of the largest investors in such assets in the euro area.

In July 2022 the ECB announced that it was taking further steps to include climate change considerations in its purchase programmes and collateral framework with the aims to better take into account climate-related financial risk in monetary policy implementation and – within its mandate – to support the green transition of the economy in line with the EU's climate neutrality objectives.

In this context, the ECB is committed to acting as a catalyst, engaging closely with the relevant EU authorities to support better and harmonised disclosure of climate-related data for assets mobilised as collateral.

Proportionate, standardised and readily accessible data Substantial efforts are already underway to improve sustainability-related transparency in securitisations.

The ESAs have been developing templates for voluntary sustainability-related disclosures for “simple, transparent and standardised” (STS) securitisations.

In March 2022, the EBA also provided guidance on how ESG standards could be implemented in the context of securitisation.

To read more:
https://www.eiopa.europa.eu/system/files/2023-03/ESAs-ECB-Joint-Statement-on-disclosures-for-securitisations-6%20March-2023.pdf

Number 5

Proposal for a regulation on Markets in Crypto-assets (MiCA)

This proposal seeks to provide legal certainty for crypto-assets not covered by existing EU financial services legislation and establish uniform rules for crypto-asset service providers and issuers at EU level. The proposed Regulation will replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation and also establish specific rules for so-called 'stablecoins', including when these are e-money. The proposed Regulation is divided into nine Titles.

Title I sets the subject matter, the scope and the definitions. Article 1 sets out that the Regulation applies to crypto-asset service providers and issuers, and establishes uniform requirements for transparency and disclosure in relation to issuance, operation, organisation and governance of crypto-asset service providers, as well as establishes consumer protection rules and measures to prevent market abuse.

Article 2 limits the scope of the Regulation to crypto-assets that do not qualify as financial instruments, deposits or structured deposits under EU financial services legislation.

Article 3 sets out the terms and definitions that are used for the purposes of this Regulation, including 'crypto-asset', 'issuer of crypto-assets', 'asset-referenced token' (often described as 'stablecoin'), 'e-money token' (often described as 'stablecoin'), 'crypto-asset service provider', 'utility token' and others.

Article 3 also defines the various crypto-asset services. Importantly, the Commission may adopt delegated acts to specify some technical elements of the definitions, to adjust them to market and technological developments.

Title II regulates the offerings and marketing to the public of crypto-assets other than asset-referenced tokens and e-money tokens.

It indicates that an issuer shall be entitled to offer such crypto-assets to the public in the Union or seek an admission to trading on a trading platform for such crypto-assets if it complies with the requirements of Article 4, such as the obligation to be established in the form of a legal person or the obligation to draw up a crypto-asset white paper in accordance with Article 5 (with Annex I) and the notification of such a crypto-asset white paper to the competent authorities (Article 7) and its publication (Article 8).

Once a whitepaper has been published, the issuer of crypto-assets can offer its crypto-assets in the EU or seeks an admission of such crypto-assets to trading on a trading platform (Article 10).

Article 4 also includes some exemptions from the publication of a whitepaper, including for small offerings of crypto-assets (below €1 million within a twelve-month period) and offerings targeting qualified investors as defined by the Prospectus Regulation (Regulation EU 2017/1129).

Article 5 and Annex I of the proposal set out the information requirements regarding the crypto-asset white paper accompanying an offer to the public of crypto-assets or an admission of crypto-assets to a trading platform for crypto-assets, while Article 6 imposes some requirements related to the marketing materials produced by the issuers of crypto-assets, other than asset-referenced tokens or e-money tokens.

The crypto-asset white paper will not be subject to a pre-approval process by the national competent authorities (Article 7). It will be notified to the national competent authorities with an assessment whether the crypto-asset at stake constitutes a financial instrument under the Markets in Financial Instruments Directive (Directive 2014/65/EU), in particular.

After the notification of the crypto-asset white paper, competent authorities will have the power to suspend or prohibit the offering, require the inclusion of additional information in the crypto-asset white paper or make public the fact that the issuer is not complying with the Regulation (Article 7).

Title II also includes specific provisions on the offers of crypto-assets that are limited in time (Article 9), the amendments of an initial crypto-asset white paper (Article 11), the right of withdrawal granted to acquirers of crypto-assets (Article 12), the obligations imposed on all issuers of crypto-assets (Article 13) and on the issuers' liability attached to the crypto-asset white paper (Article 14).

Title III, Chapter 1 describes the procedure for authorisation of asset-referenced token issuers and the approval of their crypto-asset white paper by national competent authorities (Articles 16 to 19 and Annexes I and II). To be authorised to operate in the Union, issuers of asset-referenced tokens shall be incorporated in the form of a legal entity established in the EU (Article 15).

Article 15 also indicates that no asset-referenced tokens can be offered to the public in the Union or admitted to trading on a trading platform for crypto-assets if the issuer is not authorised in the Union and it does not

publish a crypto-asset white paper approved by its competent authority. Article 15 also includes exemptions for small-scale asset-referenced tokens and for asset-referenced tokens that are marketed, distributed and exclusively held by qualified investors. Withdrawal of an authorisation is detailed in Article 20 and Article 21 sets out the procedure for modifying the crypto-asset white paper.

Title III, Chapter 2 sets out the obligations for issuers of asset-referenced tokens. It states they shall act honestly, fairly and professionally (Article 23). It lays down the rules for the publication of the crypto-asset white paper and potential marketing communications (Article 24) and the requirements for these communications (Article 25). Further, issuers are subject to ongoing information obligations (Article 26) and they are required to establish a complaint handling procedure (Article 27).

They shall also comply with other requirements, such as rules on conflicts of interest (Article 28), notification on changes to their management body to its competent authority (Article 29), governance arrangements (Article 30), own funds (Article 31), rules on the reserve of assets backing the asset-referenced tokens (Article 32) and requirements for the custody of the reserve assets (Article 33).

Article 34 explains that an issuer shall only invest the reserve assets in assets that are secure, low risk assets. Article 35 also imposes on issuers of asset-referenced tokens the disclosure of the rights attached to the asset-referenced tokens, including any direct claim on the issuer or on the reserve of assets. Where the issuer of asset-referenced tokens does not offer direct redemption rights or claims on the issuer or on the reserve assets to all holders of asset-reference tokens, Article 35 provides holders of asset-referenced tokens with minimum rights. Article 36 prevents issuers of asset-referenced tokens and crypto-asset service providers from granting any interest to holders of asset-referenced tokens.

Title III, Chapter 4, sets out the rules for the acquisition of issuers of asset-referenced tokens, with Article 37 detailing the assessment of an intended acquisition, and Article 38 the content of such an assessment.

Title III, Chapter 5, Article 39 sets out the criteria that EBA shall use when determining whether an asset-referenced token is significant. These criteria are: the size of the customer base of the promoters of the asset-referenced tokens, the value of the asset-referenced tokens or their market capitalisation, the number and value of transactions, size of the reserve of assets, significance of the issuers' cross-border activities and the interconnectedness with the financial system.

Article 39 also includes an empowerment for the Commission to adopt a delegated act in order to specify further the circumstances under which and thresholds above which an issuer of asset-referenced tokens will be considered significant. Article 39 includes some minimum thresholds that the delegated act shall in any case respect.

Article 40 details the possibility for an issuer of an asset-referenced token to classify as significant at the time of applying for an authorisation on their own initiative. Article 41 lists the additional obligations applicable to issuers of significant asset-referenced tokens, such as additional own funds requirements, liquidity management policy and interoperability.

Tittle III, Chapter 6, Article 42 obliges the issuer to have a procedure in place for an orderly wind-down of their activities.

Title IV, Chapter 1 describes the procedure for authorisation as an issuer of e-money tokens. Article 43 describes that no e-money tokens shall be offered to the public in the Union or admitted to trading on a crypto-asset trading platform unless the issuer is authorised as a credit institution or as an 'electronic money institution' within the meaning of Article 2(1) of Directive 2009/110/EC. Article 43 also states that 'e-money tokens' are deemed electronic money for the purpose of Directive 2009/110/EC.

Article 44 describes how holders of e-money tokens shall be provided with a claim on the issuer: e-money tokens shall be issued at par value and on the receipt of funds, and upon request by the holder of e-money tokens, the issuers must redeem them at any moment and at par value. Article 45 prevents issuers of e-money tokens and crypto-asset service providers from granting any interest to holders of e-money tokens.

Article 46 and Annex III sets out the requirements for the crypto-asset white paper accompanying the issuance of e-money tokens, for example: description of the issuer, detailed description of the issuer's project, indication of whether it concerns an offering of e-money tokens to the public or admission of these to a trading platform, as well as information on the risks relating to the e-money issuer, the e-money tokens and the implementation of any potential project.

Article 47 includes provision on the liability attached to such crypto-asset white paper related to e-money tokens. Article 48 sets requirements for potential marketing communications produced in relation to an offer of e-money tokens and Article 49 states that any funds received by an issuer in exchange for e-money tokens, shall be invested in assets denominated in the same currency as the one referenced by the e-money token.

Title IV, Chapter 2, Article 50 states that the EBA shall classify e-money tokens as significant on the basis of the criteria listed in Article 39. Article 51 details the possibility of an issuer of an e-money token to classify as significant at the time of applying for an authorisation on their own initiative. Article 52 contains the additional obligations applicable to issuers of significant e-money tokens. Issuers of significant e-money tokens must apply Article 33 on the custody of the reserve assets and Article 34 on the investment of these assets instead of Article 7 of Directive 2009/110/EC, Article 41, paragraphs 1, 2, and 3 on remuneration, interoperability and liquidity management, Article 41, paragraph 4 instead of Article 5 of Directive 2009/110/EC and Article 42 on an orderly wind-down of their activities.

To read more:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0593&from=EN

Number 6

Remarks at the IIB Annual Washington Conference "Trust and Global Banking: Lessons for Crypto".

Acting Comptroller of the Currency Michael J. Hsu.

Office of the Comptroller of the Currency

Thank you for inviting me to the 2023 Institute of International Bankers (IIB) Annual Washington Conference. It is a pleasure and an honor to be here.

I would like to speak today about what it takes to build and maintain trust in global banking and what lessons this may hold for crypto. In particular, I believe there are strong parallels between FTX and the Bank of Credit and Commerce International – better known in bank regulatory circles as BCCI – which failed in 1991 and led to significant changes in how global banks are supervised.

Let me start by highlighting key features of the trust architecture for global banking that has been constructed over the past several decades. That will lead to a discussion of BCCI, parallels to FTX, and lessons for crypto.

Trust in Global Banking Banking is global, while bank regulation and supervision are local. This creates challenges for bank regulators located in different jurisdictions tasked with ensuring the safety and soundness of different parts of global banks.

There are two key risks.

First, there is the risk of an unlevel playing field – where rules differ by jurisdiction – which can enable regulatory arbitrage by banks and drive races to the bottom by local authorities.

Second, there is the risk of regulators having limited visibility into and influence over global banks – what one might call "supervisability" risk. Host and home regulators, having differing lines of sight and authorities into different entities within a global bank, may struggle to see the true risk profile of the enterprise and may be limited in their abilities to address gaps.

The risk of an unlevel playing field can be mitigated by coordination among home and host authorities, while the supervisability risk of global banks can only be solved through collaboration.

To read more:
https://www.ots.treas.gov/news-issuances/speeches/2023/pub-speech-2023-23.pdf

Number 7

Statement on Silicon Valley Bank

Bank of England

The Bank of England (Bank), in consultation with the Prudential Regulation Authority (PRA), HM Treasury (HMT) and the Financial Conduct Authority (FCA), has taken the decision to sell Silicon Valley Bank UK Limited ('SVBUK'), the UK subsidiary of the US bank, to HSBC UK Bank Plc (HSBC). HSBC is authorised and supervised by the PRA and the FCA. This action has been taken to stabilise SVBUK, ensuring the continuity of banking services, minimising disruption to the UK technology sector and supporting confidence in the financial system.

The Bank and HMT can confirm that all depositors' money with SVBUK is safe and secure as a result of this transaction. SVBUK's business will continue to be operated normally by SVBUK. All services will continue to operate as normal and customers should not notice any changes.

Customers can continue to contact SVBUK through the usual channels and borrowers should make any loan repayments to SVBUK as normal. SVBUK staff remain employed by SVBUK, and SVBUK continues to be a PRA/FCA authorised bank.

Today's announcement supersedes the Bank's 10 March statement (picture below) that, absent any meaningful further information, it intended to apply to the Court to place SVBUK into a Bank Insolvency Procedure.

The Bank of England, absent any meaningful further information, intends to apply to the Court to place Silicon Valley Bank UK Limited ('SVBUK') into a Bank Insolvency Procedure. A Bank Insolvency Procedure would mean that eligible depositors are paid out by the FSCS as quickly as possible up to the protected limit of £85,000 or up to £170,000 for joint accounts. SVBUK's other assets and liabilities would be managed in the insolvency by the bank liquidators and recoveries distributed to its creditors. SVBUK has a limited presence in the UK and no critical functions supporting the financial system. In the interim, the firm will stop making payments or accepting deposits.

Given the emergence of a credible purchaser for SVBUK the Bank has determined that using its resolution powers for stabilising failing banks is appropriate.

No other UK banks are directly materially affected by these actions, or by the resolution of SVBUK's US parent bank. The wider UK banking system remains safe, sound, and well capitalised.

To read more:
https://www.bankofengland.co.uk/news/2023/march/statement-on-silicon-valley-bank

Number 8

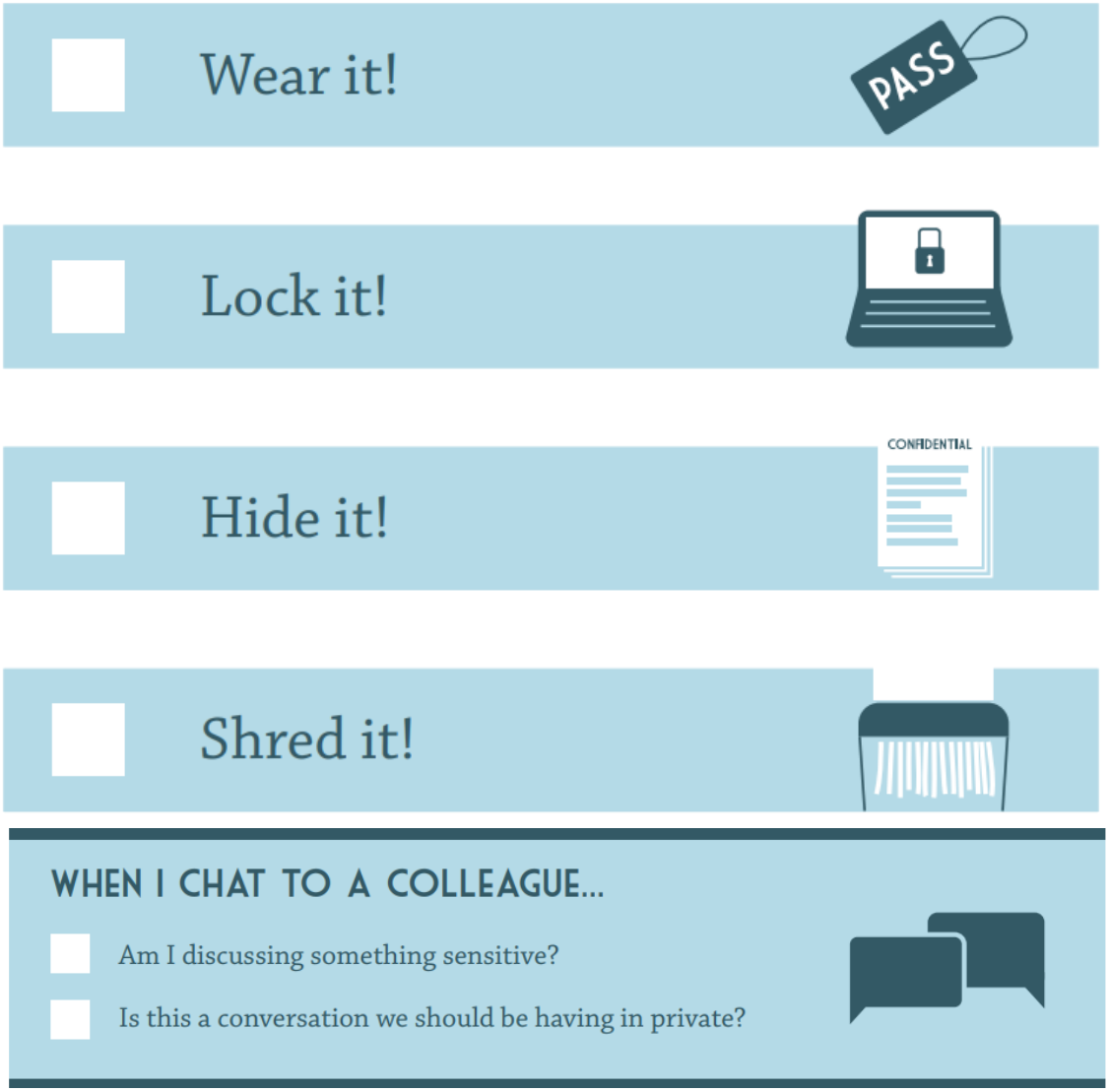
NPSA is the UK Government's National Technical Authority for Physical and Personnel Protective Security.

Security Campaigns

National Protective Security Authority

The NPSA works with partners in government, police, industry and academia to reduce the vulnerability of the national infrastructure.

NPSA has developed a series of security awareness campaigns, designed to provide organisations with a complete range of materials they need.



3.What would you do if you overheard a discussion, which you knew to be about some highly sensitive and confidential information, being held in a corridor where external visitors often pass through?

A – Approach the individuals and ask them to stop the discussion immediately – they risk compromising the security of highly sensitive information.

B – Point out where the nearest vacant meeting room is and politely suggest they continue their conversation privately in there.

C – Not say anything at the time, but make a note of the individuals involved, what they discussed, before informing either your line manager, their line manager or a security representative.

D – Remind the individuals that visitors frequent the corridor and suggest they continue their discussion elsewhere or at another time.

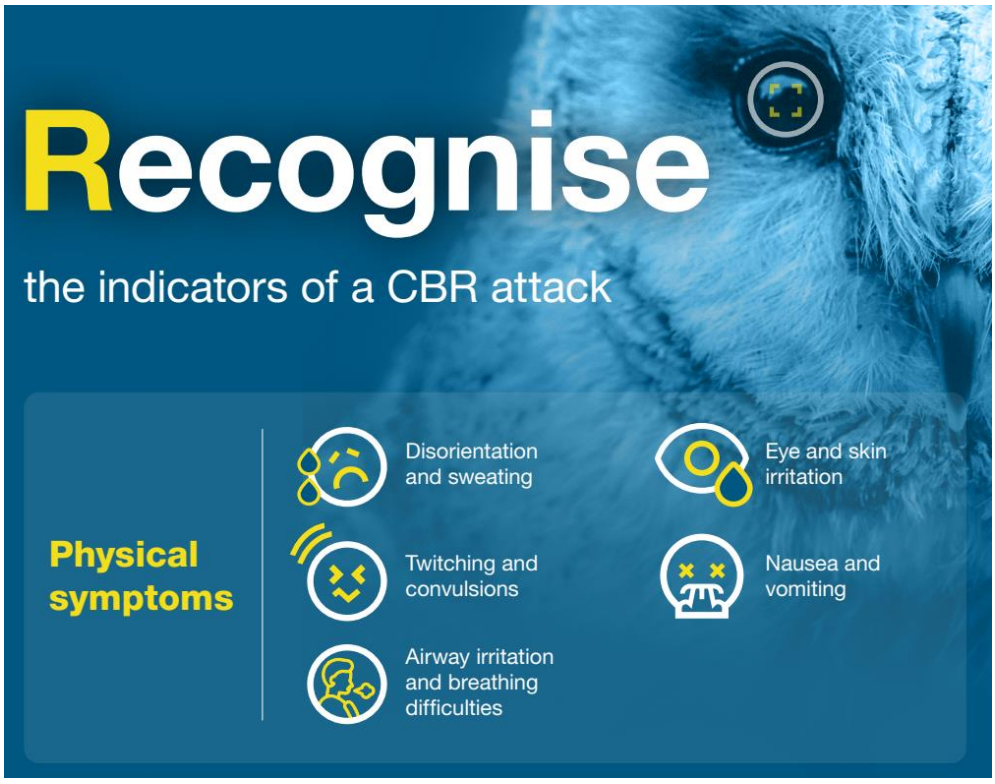
6. You notice that a colleague is unusually quiet at work, and frequently ignores basic security procedures (e.g. they send sensitive information inappropriately to a supplier over email). What would you do?

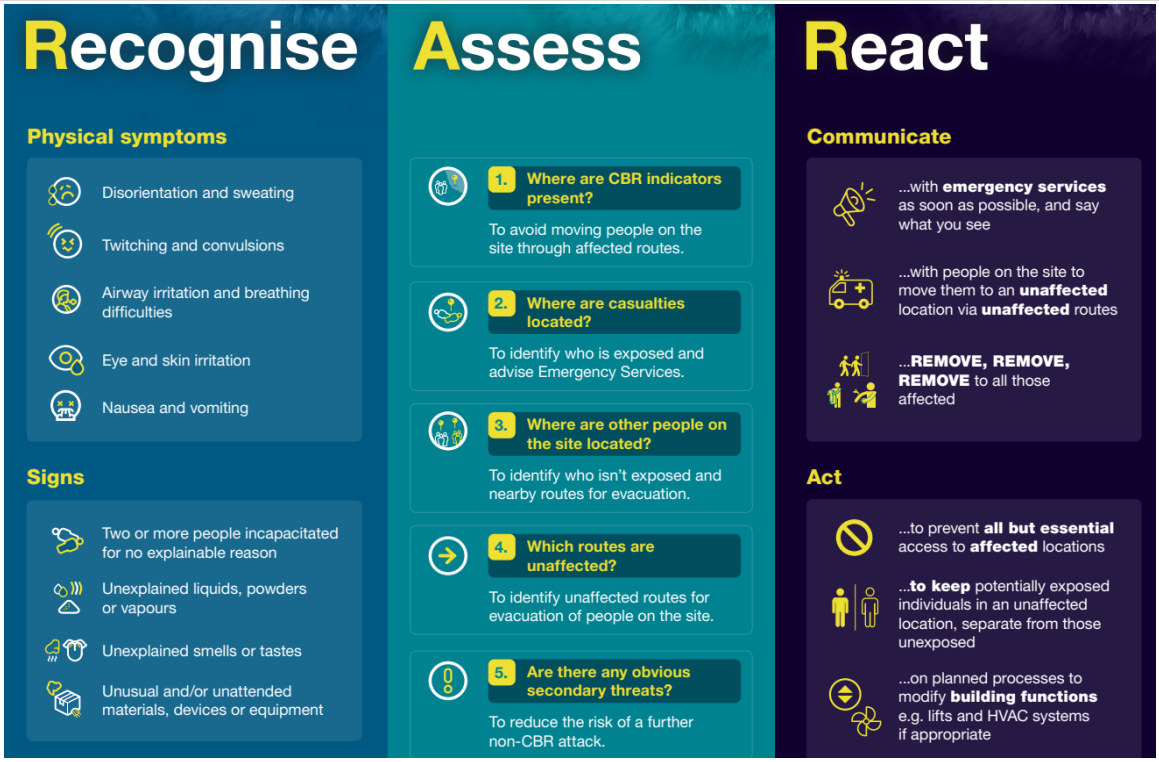
A – Let your colleague know they've been breaking security protocol and brief them on how to handle sensitive information on email.

B – Check the current security policy to ensure your colleague is deviating from this. If so, send them and others concerned a reminder of the policy. Offer to help if they are unclear what to do with certain information.

C – Keep an eye on your colleague and share your observations about their change in character and recent security lapses with a line manager. Together you can discuss a way forward.

D – Invite your colleague for an informal catch-up to ask how they are. Use this as an opportunity to also tactfully let them know that you've noticed they're not following security policy, and remind them that it's important to do so.





You may visit: https://www.npsa.gov.uk/security-campaigns

Number 9

DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit

Microsoft Threat Intelligence

Microsoft

Adversary-in-the-middle (AiTM) phishing kits are part of an increasing trend that is observed supplanting many other less advanced forms of phishing.

The following diagram illustrates the AiTM phishing attack chain:

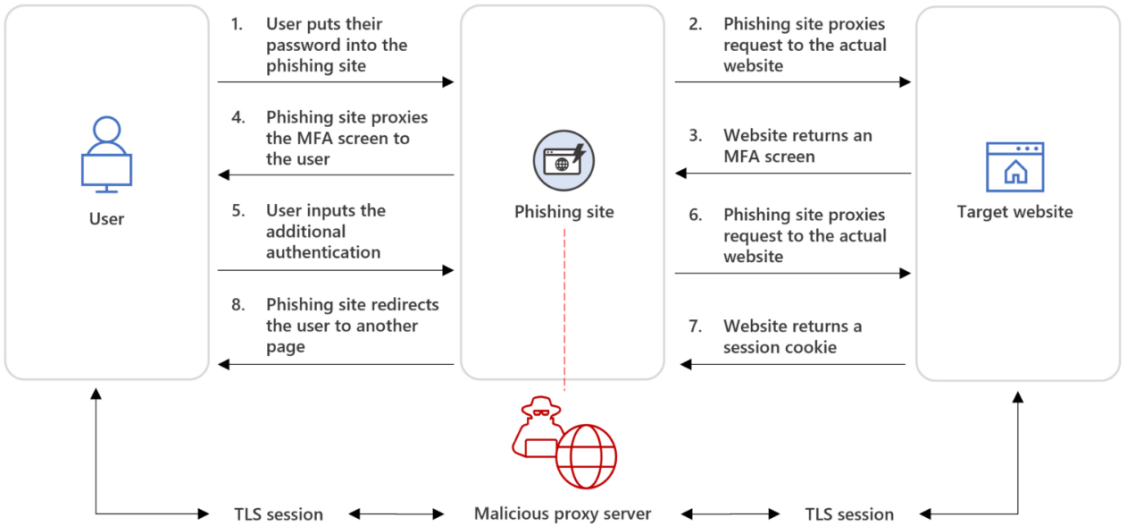


Figure 8. AiTM phishing attack diagram

AiTM phishing is capable of circumventing multifactor authentication (MFA) through reverse-proxy functionality.

DEV-1101 is an actor tracked by Microsoft responsible for the development, support, and advertising of several AiTM phishing kits, which other cybercriminals can buy or rent.

The availability of such phishing kits for purchase by attackers is part of the industrialization of the cybercriminal economy and lowers the barrier of entry for cybercrime.

DEV-1101 offers an open-source kit that automates setting up and launching phishing activity and provides support services to attackers.

The threat actor group began offering their AiTM phishing kit in 2022, and since then has made several enhancements to their kit, such as the capability to manage campaigns from mobile devices, as well as evasion features like CAPTCHA pages.

These attributes make the kit attractive to many different actors who have continually put it to use since it became available in May 2022. Actors using this kit have varying motivations and targeting and might target any industry or sector.

Microsoft 365 Defender detects suspicious activities related to AiTM phishing attacks and follow-on activities, such as session cookie theft and attempts to use the stolen cookies to sign in.

In this blog post, we share information on DEV-1101, the tool they offer, and details on related AiTM campaigns. We also share best practices and detection details to further protect organizations from AiTM phishing attacks.

AiTM tool promotion

DEV-1101 began advertising their AiTM kit around May 2022 through a Telegram channel and an advertisement in exploit[.]in, a popular cybercrime forum.

The advertisement describes the AiTM kit as a phishing application written in NodeJS with PHP reverse-proxy capabilities, automated setup, detection evasion through an antibot database, management of phishing activity through Telegram bots, and a wide range of ready-made phishing pages mimicking services such as Microsoft Office or Outlook.

On June 12, 2022, DEV-1101 announced that the kit would be open source with a $100 monthly licensing fee. The actor also provided links to additional Telegram channels and a now-defunct GitHub page.

In September 2022, DEV-1101 added the ability to manage servers running their kit through a Telegram bot rather than requiring the use of cPanel, further facilitating phishing activities and letting their customers manage campaigns from mobile devices.

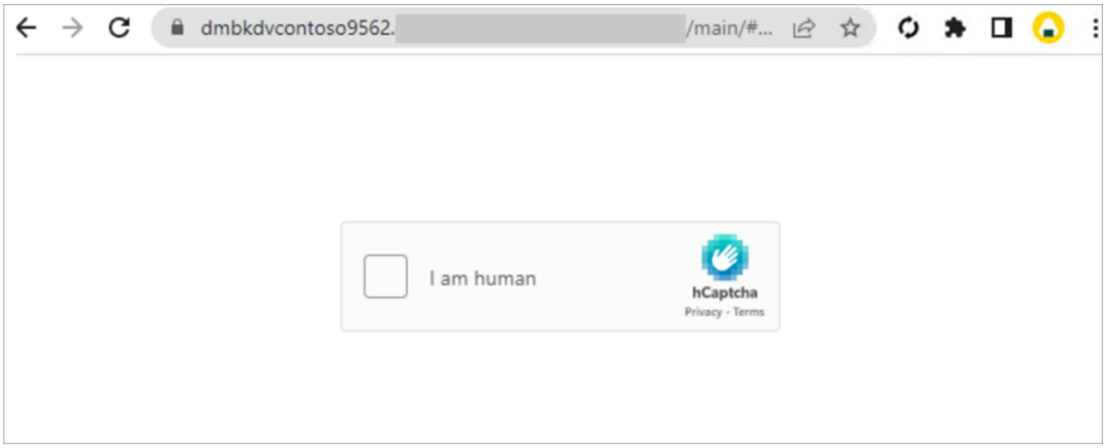
DEV-1101 was able to increase the price of their tool multiple times due to the rapid growth of their user base from July through December 2022. This allowed DEV-1101 to dedicate themselves fully to the development and support of their tool.

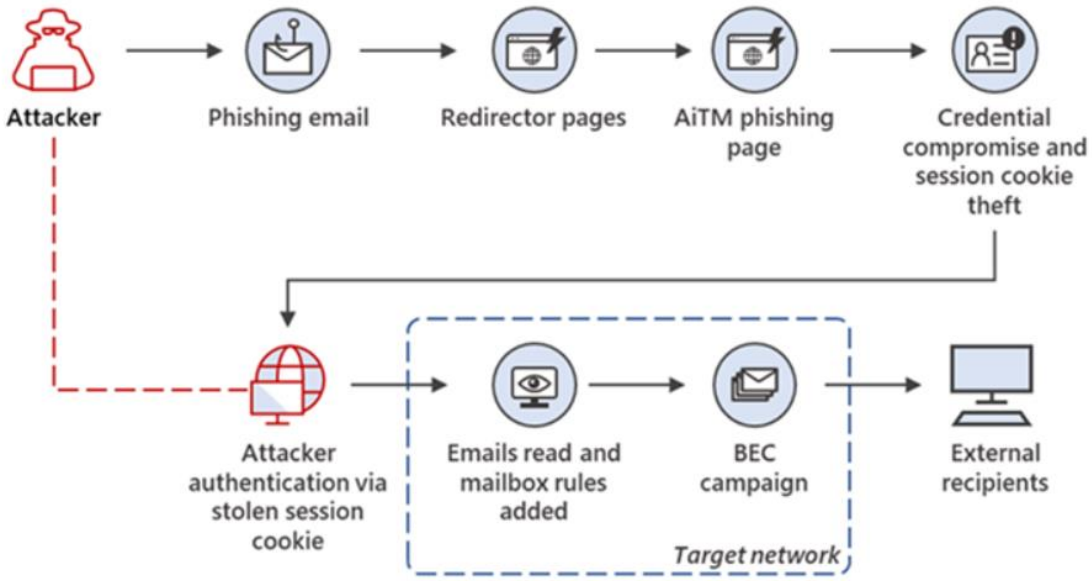
As of this writing, DEV-1101 offers their tool for $300, with VIP licenses at $1,000. Legacy users were permitted to continue purchasing licenses at $200 prior to January 1, 2023.

Microsoft observed several high-volume phishing campaigns from various actors using the tool offered by DEV-1101, comprising millions of phishing emails per day.

DEV-0928, an actor Microsoft has tracked since September 2022, is one of DEV-1101's more prominent patrons and was observed launching a phishing campaign involving over one million emails.

The kit also allows threat actors to use CAPTCHA to evade detection. Inserting a CAPTCHA page into the phishing sequence could make it more difficult for automated systems to reach the final phishing page, while a human could easily click through to the next page.





To read more:
https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

Number 10

Office of the Director of National Intelligence

2023 Annual Threat Assessment of the U.S. Intelligence Community

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the Intelligence Authorization Act (Pub. L. No. 116-260).

This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC.

All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future.

Information available as of 18 January was used in the preparation of this assessment.

China, Cyber

China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks.

China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland, suppression of the free flow of information in cyberspace—such as U.S. web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally.

If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide.

Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.

- China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.

China leads the world in applying surveillance and censorship to monitor its population and repress dissent. Beijing conducts cyber intrusions that are targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of CCP narratives, policies, and actions.

- China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

China, malign influence operations

Beijing will continue expanding its global intelligence and covert influence posture to better support the CCP's political, economic, and security goals.

China is attempting to sow doubts about U.S. leadership, undermine democracy, and extend Beijing's influence, particularly in East Asia and the western Pacific, which Beijing views as its sphere of influence.

Beijing largely concentrates its U.S.-focused influence efforts on shaping U.S. policy and the U.S. public's perception of China in a positive direction, but has shown a willingness to meddle in select election races that involved perceived anti-China politicians.

- Beijing uses a sophisticated array of covert, overt, licit, and illicit means to try to soften U.S. criticism, shape U.S. power centers' views of China, and influence policymakers at all levels of government.

PRC leaders probably believe that a U.S. bipartisan consensus against China is impeding their efforts to directly influence U.S. national-level policy regarding China.

Beijing has adjusted by redoubling its efforts to build influence at the state and local level to shift U.S. policy in China's favor because of Beijing's belief that local officials are more pliable than their federal counterparts.

PRC actors have become more aggressive with their influence campaigns, probably motivated by their view that antiChina sentiment in the United States is threatening their international image, access to markets, and technological expertise.

Beijing's growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow's playbook for influence operations.

- Beijing is intensifying efforts to mold U.S. public discourse—particularly by trying to shape U.S. views of sensitive or core sovereignty issues, such as Taiwan, Xinjiang, Tibet, and Hong Kong—and pressure perceived political opponents.

As part of efforts to stifle anti-Beijing criticism, the PRC monitors overseas Chinese students for dissident views, mobilizes Chinese student associations to conduct activities on behalf of Beijing, and influences research by U.S. academics and think tank experts.

These activities have included pressuring family members in China, denying or canceling visas, blocking access to China's archives and resources, and disrupting or withdrawing funding for exchange programs.

- China is rapidly expanding and improving its artificial intelligence (AI) and big data analytics capabilities, which could expand beyond domestic use.

Russia, Cyber

The Ukraine war was the key factor in Russia's cyber operations prioritization in 2022.

Although its cyber activity surrounding the war fell short of the pace and impact we had expected, Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.

Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions.

- Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems,

in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.

Russia, malign influence operations

Russia presents one of the most serious foreign influence threats to the United States, because it uses its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances and increase its sway around the world, while attempting to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and decisionmaking.

Moscow probably will build on these approaches to try to undermine the United States as opportunities arise.

Russia and its influence actors are adept at capitalizing on current events in the United States to push Moscow-friendly positions to Western audiences.

Russian officials, including Putin himself, and influence actors routinely inject themselves into contentious U.S. issues, even if that causes the Kremlin to take a public stand on U.S. domestic political matters.

- Moscow views U.S. elections as opportunities for malign influence as part of its larger foreign policy strategy. Moscow has conducted influence operations against U.S. elections for decades, including as recently as the U.S. midterm elections in 2022. It will try to strengthen ties to U.S. persons in the media and politics in hopes of developing vectors for future influence operations.

- Russia's influence actors have adapted their efforts to increasingly hide their hand, laundering their preferred messaging through a vast ecosystem of Russian proxy websites, individuals, and organizations that appear to be independent news sources.

Moscow seeds original stories or amplifies preexisting popular or divisive discourse using a network of state media, proxy, and social media influence actors and then intensifies that content to further penetrate the Western information environment.

These activities can include disseminating false content and amplifying information perceived as beneficial to Russian influence efforts or conspiracy theories.

DEVELOPMENTS IN TECHNOLOGY

New technologies—particularly in the fields of AI and biotechnology—are being developed and are proliferating faster than companies and governments can shape norms, protect privacy, and prevent dangerous outcomes.

The convergence of emerging technologies is likely to create potentially breakthrough technologies not foreseeable by examining narrow science and technology areas, which could lead to the rapid development of asymmetric threats to U.S. interests.

• The convergence of capabilities in high-performance computing, big data, and machine learning—each a critical enabler across multiple domains—could have broad yet unidentified consequences across military, commercial, and basic research applications with relevance to national defense, economic security, and political stability.

• Large-scale simulation and the accumulation and analysis of massive amounts of data are revolutionizing many areas of science and engineering research with the potential to influence the future battlefield and shape political discourse through disinformation operations.

Our adversaries increasingly view data as a strategic resource. They are focused on acquiring and analyzing data—from personally identifiable information on U.S. citizens to commercial and government data—that can make their espionage, influence, kinetic and cyber attack operations more effective; advance their exploitation of the U.S. economy; and give them strategic advantage over the United States.

• Foreign intelligence services are adopting cutting-edge technologies —from advanced cyber tools to unmanned systems to enhanced technical surveillance equipment—that improve their capabilities and challenge U.S. defenses. Much of this technology is available commercially, providing a shortcut for previously unsophisticated services to become legitimate threats.

The global pandemic, which spurred unprecedented collection of genetic and health data worldwide, along with technological advances in genetic engineering, genome sequencing, and DNA modification, are driving new lines of effort in biotech research.

• Several countries, universities, and private companies have or are creating centralized genetic or genomic databases to collect, store, process, and

analyze genetic data, albeit at the risk of potentially compromising health and genetic data privacy, and are ripe targets for cyber attack and theft.

• China has been collecting genetic and health data from its entire population, bolstering the state's surveillance and security apparatus, and its ability to try to monitor, manage, and control society in real-time. Beijing also has collected U.S. health and genomic data through its acquisitions and investments in U.S. companies, as well as cyber breaches.

Advances in semiconductors and high-performance computing are driving military and technological breakthroughs, but also are heightening the risk of technology surprise because high-performance computers will help address longstanding research and development hurdles.

Our adversaries' advances in semiconductors and high-performance computing could result in future challenges to our military and technological sectors.

• China may now have two exascale systems using older generation, domestically designed processors— neither of which have been officially acknowledged or subject to independent benchmarks—and plans to build more by 2025.

Exascale computers are capable of solving massive scientific challenges that would have been impossible with previous generation supercomputers.

• As of June 2022, China had 173 of the world's most powerful supercomputers, a third more than the United States, which accounted for 128 supercomputers.

TRENDS IN DIGITAL AUTHORITARIANISM AND MALIGN INFLUENCE

Globally, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, further threatening to distort publicly available information and probably will outpace efforts to protect digital freedoms.

The exploitation of U.S. citizens' sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology, probably will continue to threaten U.S. interests.

Authoritarian governments usually are the principal offenders of digital repression, but some democratic states have engaged in similar approaches, contributing to democratic backsliding and erosion.

Many foreign governments have become adept at the tools of digital repression, employing censorship, misinformation and disinformation, mass surveillance, and invasive spyware to suppress freedom.

During the next several years, governments are likely to grow more sophisticated in their use of existing technologies, and learn quickly how to exploit new and more intrusive technologies for repression, particularly automated surveillance and identity resolution techniques.

• Digital repression is occurring against the backdrop of broader digital influence operations that many autocrats are conducting globally to try to shape how foreign publics view their regimes, create social and political upheaval in some democracies, shift policies, and sway voters' perspectives and preferences.

Various technologies now constitute an important component of many governments' repressive toolkits, extending states' power to stifle dissent beyond traditional means—such as censoring print media or physically harming dissidents—which repressive regimes continue to employ.

Firms around the world sell capabilities and expertise that facilitate governments' internal and extraterritorial monitoring and repression.

• The commercial spyware industry—which makes tools that allow users to hack digital devices such as mobile telephones to surveil users—grew rapidly during the past decade and is now estimated to be worth $12 billion.

While some states use such spyware tools and lawful intercept programs to target criminals and terrorists, governments also are increasingly using spyware to target political opposition and dissidents.

• Authoritarian states use spyware and other digital means to conduct transnational repression against individual critics and diaspora communities to limit their influence over domestic audiences.

Monitoring and threats against these communities limit freedom of speech wherever they reside, including in the United States and other liberal democracies.

• Beijing has demonstrated its willingness to enlist the aid of China-based commercial enterprises to help surveil and censor PRC critics abroad, and China's technology industry is a key global supplier of advanced surveillance technologies to foreign governments.

The report:
https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.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,

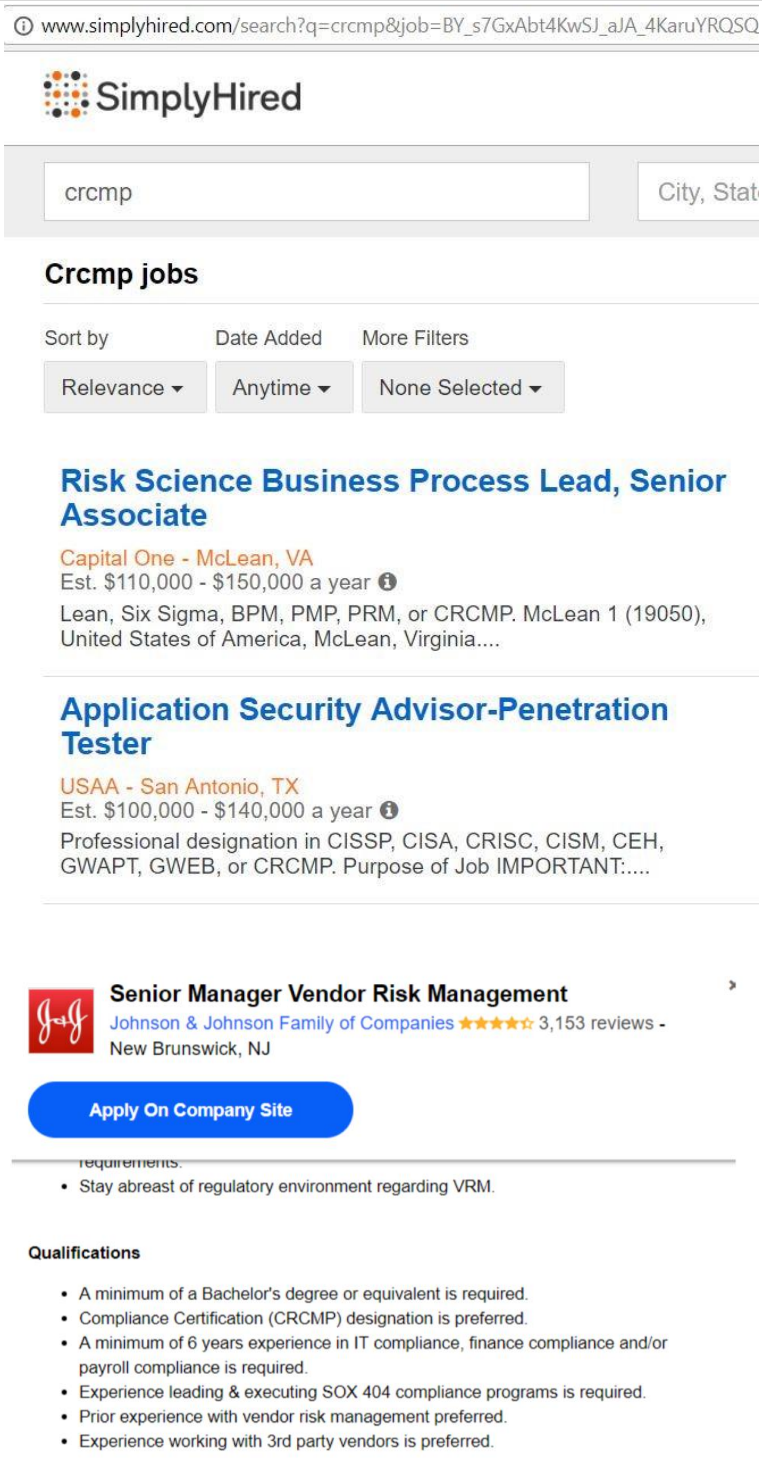
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- 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.